Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2002-06

Centeralizing to achieve information superiority

Voce, Russell S.

Monterey, California ; Naval Postgraduate School

http://hdl.handle.net/10945/5904

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

CENTERALIZING TO ACHIEVE INFORMATION SUPERIORITY

by

Terry L. Jordan
Russell S. Voce

June 2002

Thesis Advisor:	Dan C. Boger
Second Reader:	Erik Jansen

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) **CENTERALIZING TO ACHIEVE INFORMATION SUPERIORITY**			**5. FUNDING NUMBERS**
6. AUTHOR(S) Jordan, Terry L. and Voce, Russell S			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT ***(maximum 200 words)***

The purpose of this thesis is to propose a potential organizational structure for effectively utilizing Information Operations (IO) within the Department of Defense (DOD). This thesis is in response to a request for research from the vice commander of the 193 Special Operations Wing. According to this individual, the FY 1999 Joint Warfighting Capabilities Assessment, IO panel cycle, highlighted various deficiencies ranging from inadequate manning and force structure, to ineffective planning and integration processes, to inadequate capabilities available to support CINC requirements. Currently no one federal agency or military department has total responsibility or authority to bring all the disparate, but dependent, IO functions/requirements together. As a result, funding, personnel resourcing, and control is fragmented to the detriment of the nation's warfighting capabilities. As demonstrated by the above finding, the subject of IO has pervaded numerous warfighting commands, doctrinal documents, and future vision plans. Despite this pervasion, there is no single agency within DOD that has the sole responsibility for providing or prosecuting information operations. The thesis will answer the question: What is an effective organizational structure for providing information operations that produces the synergistic effects of centralization without reducing the gains achieved at unit levels by having a decentralized approach? The answer to this question will provide an organizational model that may be applied to any individual service, or DOD as a whole, to provide an organized approach to IO. The authors of this thesis do not contend that this model will be the only way to organize for IO, only one way to organize for IO.

14. SUBJECT TERMS Information Operations, Organizational Modeling, C4ISR Command and Control			**15. NUMBER OF PAGES** 98
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

CENTERALIZING TO ACHIEVE INFORMATION SUPERIORITY

Terry L. Jordan - Major, United States Air Force
B.S., Air Force Academy, 1985
M.S., Troy State University, 1994

Russell S. Voce - Captain, United States Air Force
B.S., University of Southern Mississippi, 1993

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
DEFENSE ANALYSIS**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2002**

Authors: Terry L. Jordan

Russell S. Voce

Approved by: Dan Boger
Thesis Advisor

Eric Jansen
Second Reader/Co-Advisor

Gordon McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to propose a potential organizational structure for effectively utilizing Information Operations (IO) within the Department of Defense (DOD). This thesis is in response to a request for research from the vice commander of the 193 Special Operations Wing. According to this individual, the FY 1999 Joint Warfighting Capabilities Assessment, IO panel cycle, highlighted various deficiencies ranging from inadequate manning and force structure, to ineffective planning and integration processes, to inadequate capabilities available to support CINC requirements. Currently no one federal agency or military department has total responsibility or authority to bring all the disparate, but dependent, IO functions/requirements together. As a result, funding, personnel resourcing, and control is fragmented to the detriment of the nation's warfighting capabilities.

As demonstrated by the above finding, the subject of IO has pervaded numerous warfighting commands, doctrinal documents, and future vision plans. Despite this pervasion, there is no single agency within DOD that has the sole responsibility for providing or prosecuting information operations. The thesis will answer the question: What is an effective organizational structure for providing information operations that produces the synergistic effects of centralization without reducing the gains achieved at unit levels by having a decentralized approach? The answer to this question will provide an organizational model that may be applied to any individual service, or DOD as a whole, to provide an organized approach to IO. The authors of this thesis do not contend that this model will be the only way to organize for IO, only one way to organize for IO.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. OVERVIEW 1
B. METHODOLOGY 1

II. WHY AN ORGANIZATIONAL CHANGE? 3
A. INTRODUCTION 3
B. PROBLEMS 3
C. SOLUTIONS FOR CHANGE 9
D. ORGANIZATIONAL APPROACH 10
E. GOALS OF A NEW IO COMMAND 12
F. CONCLUSION 15

III. WHAT CAUSES ORGANIZATIONAL CENTRALIZATION IN DOD? 17
A. INTRODUCTION 17
B. SELECTED CASES AND WHY 17
C. INDEPENDENT VARIABLES 19
D. ANALYSIS—USAF 21
E. ANALYSIS—USSOCOM 25
F. ANALYSIS—NORTHCOM 30
G. ANALYSIS—AIR CORPS FOLLOWING WWI 31
H. CONCLUSION—INFORMATION OPERATIONS (IO) COMMAND 31

IV. AN INFORMATION OPERATIONS ORGANIZATIONAL STRUCTURE MODEL 35
A. INTRODUCTION 35
B. TERMS 35
C. THE STRUCTURE 36
D. LEGAL 37
E. FUTURE CONCEPTS 38
F. COMMERCIAL INTERFACE 38
G. PUBLIC AFFAIRS 39
H. PRODUCT DEVELOPMENT/DISTRIBUTION 40
I. CORPORATE SUPPORT 41
J. OPERATIONS 44
K. CONCLUSION 46

V. AN APPLICATION OF THE MODEL 47
A. INTRODUCTION 47
B. LEGAL 47
C. FUTURE CONCEPTS 48
D. COMMERCIAL INTERFACE 49
E. PUBLIC AFFAIRS (PA) 50
F. CORPORATE SUPPORT 50
1. Joint Spectrum Center (JSC) 50
2. Joint Warfare Analysis Center (JWAC) 51
3. Service Components 51

G. PRODUCT DEVELOPMENT/DISTRIBUTION 52
H. OPERATIONS 54
1. Combat Support Package(s) 54
2. Information Operations Computer Emergency Response Team (IOCERT) 55
I. DIVISIONAL LIAISONS 56
J. INTERRELATION WITH OTHER DOD AGENCIES 57
1. Defense Information Systems Agency (DISA) 57
2. National Reconnaissance Office (NRO) 57
3. National Security Agency (NSA) 57
4. Defense Intelligence Agency (DIA) 57
5. Chairman Joint Chiefs of Staff (CJCS) 57
K. CONCLUSION 57

VI. MODELING THE MODEL: A CULTURE OF KNOWLEDGE 59
A. INTRODUCTION 59
B. ABOUT VITE 59
C. MODEL OVERVIEW 60
1. The Actors 60
2. The Activities 60
a. IO Plan 61
b. Intel Product 61
c. ROE 61
d. PSYOP Plan 62
e. CNA Plan 62
f. EW Plan 63
g. PA Plan 63
h. CA Plan 63
3. Activity Flow 63
4. The Model 64
D. SCENARIO 1 65
1. Skill Levels 65
2. Results 66
E. SCENARIO 2 67
1. Skill Levels 67
2. Results 67
F. ANALYSIS 68
G. CONCLUSION 69

VII. CONCLUSION 71
A. SUMMARY 71
B. FURTHER RESEARCH 72
1. Classified Data 72
2. Further Integration of Surveillance and Reconnaissance 73
3. Manpower Study 73
4. Fiscal Feasibility 74
5. Flattening the Hierarchy 74

LIST OF REFERENCES 75
INITIAL DISTRIBUTION LIST 79

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Elements of Marine Corps Information Operations(From: Marine Corps) 11
Figure 2. Application of Terms 36
Figure 3. IO Command Structure 37
Figure 4. Legal 37
Figure 5. Future Concepts 38
Figure 6. Commercial Interface 38
Figure 7. Public Affairs 39
Figure 8. Product Development/Distribution 40
Figure 9. Interrelation Diagram 41
Figure 10. Corporate Support 41
Figure 11. Flow of Authority/Communication 42
Figure 12. CERT Process 43
Figure 13. Operations 44
Figure 14. USIOC 48
Figure 15. IO Cell Vitae© Model 64

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Independent Variables 21
Table 2. Scenario 1 Skill Levels 66
Table 3. Scenario 1 Results 66
Table 4. Scenario 2 Skill Levels 67
Table 5. Scenario 2 Results 68
Table 6. Scenario Analysis 69

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis explores the development of an organizational model for providing Information Operations (IO) related functions at either a unified or service level of command. The main emphasis consists of justifying the reason for having the discussion, deriving a generic organizational structure, demonstrating the feasibility of implementation, and finally demonstrating the potential gains of implementation.

First, the justification for even exploring this issue is emphasized. One explanation for scrutinizing the organization of IO is centered around three elements: 1) promotion of unity of command, 2) elimination of redundancy or unity of effort, and 3) providing synergism between diverse functional areas, i.e., Intelligence, PSYOPS, PA, Communications, etc.

After highlighting the reasons to inspect the organization of IO, we offered a case study analysis concerning the causes of centralization in DOD. The cases used were: 1) formation of the USAF as a separate service, 2) establishment of USSOCOM, 3) creation of NORTHCOM following 9/11, and 4) organization of the Air Corps following World War I. These cases are matched against the possibility of a separate IO command. Several variables that add validity to IO centralization as well as other cases studied include: 1) no clear chain of command, 2) possible failure in conflict, and 3) external threat.

Since IO organization is worth examining and the organizational centralization of IO is potentially warranted in DOD, we developed a generic organizational structure by using an existing paradigm, i.e., USSOCOM. We showed how this organization would support both peace time and war time operations, how it can provide for all functional areas related to IO, and how it conducts day-to-day functions using a matrix structure throughout an existing force.

Using this generic organizational structure, we showed the application of this model at a unified level of command. This step in development demonstrates the feasibility of implementing an organizational model. It also shows how using existing organizations in DOD, i.e., JWAC, USACAPOC, etc., reduces fiscal constraints.

In the last phase of this organizational model development, we modeled a subset of the generic model using VITE© software (a form of organizational modeling software). Specifically, we modeled an IO cell tasked with developing an IO plan for a JTF commander. Overall, this demonstrates a possible IO model's synergistic effects by simulating how PSYOPS, CA, PA, Intelligence and Communications can join forces. Two scenarios are used: 1) where individuals have never worked together before and 2) where individuals have trained and worked together as part of an IO command. The results of this simulation showed that there was a minimum 50 percent improvement in task accomplishment under an IO command environment.

In conclusion, even though a separate IO command may not be the only way, it can promote the achievement of Information Superiority that is part of JV 2010, 2020, and other future doctrines.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

The purpose of this thesis is to propose a potential organizational structure for effectively utilizing Information Operations (IO) within the Department of Defense (DOD). This thesis is in response to a request for research from the vice commander of the 193 Special Operations Wing. According to this individual, the FY 1999 Joint Warfighting Capabilities Assessment, IO panel cycle, highlighted various deficiencies ranging from inadequate manning and force structure, to ineffective planning and integration processes, to inadequate capabilities available to support CINC requirements. Currently no one federal agency or military department has total responsibility or authority to bring all the disparate, but dependent, IO functions/requirements together. As a result, funding, personnel resourcing, and control is fragmented to the detriment of the nation's warfighting capabilities.

As demonstrated by the above finding, the subject of IO has pervaded numerous warfighting commands, doctrinal documents, and future vision plans. Despite this pervasion, there is no single agency within DOD that has the sole responsibility for providing or prosecuting information operations. The thesis will answer the question: What is an effective organizational structure for providing information operations that produces the synergistic effects of centralization without reducing the gains achieved at unit levels by having a decentralized approach? The answer to this question will provide an organizational model that may be applied to any individual service, or DOD as a whole, to provide an organized approach to IO. The authors of this thesis do not contend that this model will be the only way to organize for IO, only one way to organize for IO.

B. METHODOLOGY

This thesis will utilize several approaches to develop its organizational model. Several approaches are utilized due to the complexity of the question poised by this thesis.

There will first be a general discussion of the state of IO in today's military. The purpose of this discussion is to provide some justification for even exploring the creation

of an organizational model for IO. In short, it is intended to preempt the naysayers who will claim there is no reason for even discussing the topic.

Following this is the presentation of a generic organizational model for providing IO. The model is derived by examining current military organizations, i.e., the existing unified commands and major commands in the separate services. As well, the requirements for IO as set forth in Joint Pub 3-13, Joint Doctrine for Information Operations, are used. The model is intended be a template that can be applied at either the unified or individual service level.

After describing the generic model, the feasibility of implementing the model is demonstrated by applying the model at the unified command level to create the nominal organization of the United States Information Operations Command (USIOC). In order to demonstrate real-world feasibility, existing organizations are applied to the generic model.

Finally, to demonstrate the potential gains of implementing the model, a portion of the organization is modeled using the organizational modeling software Vite©. The goal of this modeling effort is to determine if there are any gains to be realized by having personnel of differing fields of expertise yet are members of the same organization work together. The contention is that by being in a single organization, a culture of knowledge will exist that allows individual members to have a higher understanding of their peer's particular field of expertise. The hope is that this higher understanding will result in improvements in working on a collaborative project that involves numerous diverse areas of expertise, i.e., an IO plan.

In short, the methodology used consists of justifying the reason for having the discussion, deriving a generic organizational structure, demonstrating the feasibility of implementation, and finally demonstrating the potential gains of implementation.

II. WHY AN ORGANIZATIONAL CHANGE?

A. INTRODUCTION

In the past, the world leisurely strolled to the front door, coffee in hand, to get the morning newspaper. However, today, the world wakes up, rolls over, and powers-up the personal computer. The World Wide Web has become the world's information source 24 hours a day, 7 days a week. The information revolution must be reckoned with as it grows exponentially. This wealth and speed of information can be exploited as an advantage during modern warfare.

> …as the US defense community debates the role of information in warfare, new information-age threats and enemies are emerging. States, even individuals, without traditional sources of military power, can threaten US global military leadership. To confront this new potential, the US armed forces must understand information power and how to organize for victory in joint warfighting. (Gortler, 1995)

To form a better, more complete understanding of Information Operations (IO) with regards to modern warfare, we must understand the problems with the U.S. military's current approach to IO. Once these problems are recognized, the question becomes what corrective actions should be taken? These corrective actions may stimulate organizational changes, such as the creation of a new IO command. In this chapter, I will explore the current problems that exist within the IO framework of DOD. I will specifically address problems associated with some basic principles of war that have proven reliable throughout military history. Once these problems are evident, I will offer some possible solutions for change to include an organizational approach that can be used to alleviate the problems and some goals that may be appropriate to "jump start" an organizational change for IO.

B. PROBLEMS

Although Desert Storm may have not been the first true "information war," it raised the awareness of military strategists to a point where IO can be considered the key to victory in future military conflicts.

> Growing evidence suggests that new military organizations and far more capable means and methods of warfare will supersede the military systems, operations, organizations, and force structures that dominated the Cold War. To maintain its lead in the Information Age, the US must truly revolutionize its military affairs. Piecemeal infusion of information-age technologies is insufficient. Such infusions certainly provided an overwhelming edge to the US during the Gulf War, but now the genie is out of the bottle. Others, nations and individuals, are pursuing information power. To revolutionize military operations, the US must radically change its organizational, operational, and doctrinal approaches. If the US military does this methodically, it will emerge from the revolution prepared to confront the formidable information-age threats posed by an expanded battlespace and non-traditional classes of warriors. (Gortler, 1995)

Commanders dating back to Sun Tzu have realized the importance of information superiority when faced with opposing forces. The publication of the first joint IO doctrine (Joint Pub 3-13) in October 1998 also demonstrates this recognition and the need for a fundamental set of guidelines in the area of IO. In relation to future conflict, what are the problems with the U.S. military's current approach to understanding the applications of IO? To begin, we should look at the U.S. military's apparent departure from one of the basic principles of war relative to IO.

One of the most fundamental principles of war described by the world-renowned war theorist, Karl von Clausewitz, is unity of command. Unity of command focuses on capabilities in support of the main objective under the leadership of one commander.

> Unity simply recognizes the fact that a committee is not best suited to making rapid decisions; that a single representative from a group, is better able to communicate with external organizations; and a clear leader is good for morale. Too many bosses breed confusion, office politics severely hampers productivity. Unity defines who is accountable for what. Unity of Command is why the executive branch is in charge of the military, there are 100s of members of Congress, there is only one Commander-in-Chief (Morgan, 2000).

In effect, the above statement describes centralization, as well; "when all the power for decision making rests at a single point in the organization-ultimately in the hands of one person-we shall call the structure centralized" (Mintzberg, 1993, p.95). Joint Pub 3-13 establishes a planning and coordinating IO cell to support the Joint Force

Commanders. However, a problem arises because there is no single entity responsible for IO as is the case with other J-n roles, such as J-6 (Communications) or J-3 (Operations). The IO cell reports to operations, but does not include intelligence or communication efforts directly, which are merely coordination related.

> The current arrangement on the Joint Staff presents some unique challenges as no one is actually in charge. J-3 and J-6 are too busy to dedicate the constant attention this area requires and day-to-day responsibility for IO on the Joint Staff is delegated. A need exists for direct flag officer sponsorship to orchestrate joint IO policy and doctrine development, conduct operational planning, and establish requirements. (Fredericks, 1997)

This point is also emphasized when one looks at the IO structure of the U.S. Air Force.

Current Air Force (AF) structure has three major players in the IO arena: the Air Intelligence Agency (AIA), the Air Force Communication Agency (AFCA), and the Chief Information Officer (CIO). First, and probably foremost, is AIA whose mission, in part, is to "provide full-spectrum information operations products, applications, services and resources to Air Force major commands" (Air Intelligence, 2000). AIA was previously a Field Operating Agency of the Air Staff, but as of February 1, 2001, the organization was rolled into the Air Combat Command (ACC). The AFCA has a similar mission in part, where it is tasked with "helping the Air Force maintain information superiority by ensuring that communications and information systems used by the war fighters are integrated and interoperable" (Air Force, 2000). While the AFCA has no structural link to AIA other than being in the AF, it does report to the deputy CIO. The CIO's vision, similar to a mission, is "an Air Force that works better and costs less through the smart use of information" (Visions, 2000). In short, the CIO and AFCA are players within the communications functional community, whereas AIA is owned and predominately run by the intelligence community. As stated before, other than all being in the AF, there is no structural organization that ties all parties together, and therein lies a major portion of the problem.

It seems there will be a need for some decentralization when and if an IO command is established, because of its need "to respond quickly to local conditions" and because it cannot possibly make all its decisions "at one center" within the rapidly

changing information environment (Mintzberg, p.96). The U.S. military can obtain the benefits of centralization as well as decentralization. Each approach is not a fixed solution, since they can and do operate on a continuous scale. However, there needs to be a means to achieve overall coordination and direction that a centralized structure may be able to provide.

Up to this point, DOD IO activities can be characterized as highly decentralized with no single person "in charge" which leads to another dilemma in a key element of war - objective. According to FM 100-5, every military endeavor should be directed towards a clearly defined, decisive, and attainable objective (1994). Although DOD has fashioned various, all-encompassing definitions for IO and what it includes, there is no instrument for developing, integrating, and maintaining strategic IO initiatives. Currently DOD's answer to IO command and control is spread throughout agencies, unified commands, JTF organizations and individual services. Consequentially, the overall "belly button" for IO seems to lie with the SECDEF's Chief Information Officer (CIO). Although the DOD CIO is "responsible for providing capabilities that enable the military forces of the United States to generate, use and share information necessary to survive and succeed on every mission" (ASD C3I, 2001), he has not defined or explained IO in unambiguous terms. This state in IO affairs has not prompted the establishment of a concise objective, which the "leader in charge" should provide. Also, without a defined objective, DOD tends to reiterate work that has already been accomplished or wastefully spend dollars on systems or methods already being utilized.

The above-mentioned decentralized approach brings us to the last problem associated with the military's approach to understanding IO. In operation, this distributed scheme and lack of command within the defense community is causing a problem with the "economy of force" principle of war. While every DOD organization is vying for the prestige of becoming the "go to" expert in IO, duplication of effort is rampant, which can lead to unnecessary dispersal of scarce funds needed in all areas of information warfare. Instead of minimizing its endeavors concerning IO matters, each service, command or organization is exuding tremendous effort. Individual commands, branches of service and units are allowed flexibility to employ IO in manners best suited to their unique requirements. The DOD CIO structure in place offers little guidance to capitalize on

individual advances in IO such that there is corporate advancement in the area of IO. Each service has formed its own IO strategy to outline direction, doctrine and objectives within the IO realm and lack any coordinating mechanisms to learn from each other. While this decentralized approach has allowed organizational learning that more fully explores an unknown arena, it also has allowed the services to engage in independent corporate advancement, which may not be to the benefit of the overall IO "jointness" of the defense department. The notion of corporate advancement, laying claim to new concepts in order to gain additional funds, recognition and prestige is even evident within the individual services.

As an example, both the Navy and the Army conducted exercises using cutting edge technology to demonstrate the capability to enhance the operations of conventional forces with technology. In both exercises similar, yet different, technology was used (Adams, J., p. 119). Basically, two separate services traveled down two different paths to get to the same location, and both paths were toll roads. Similar to this case, both the Air Force Information Warfare Center and the Fleet Information Warfare Center use systems to monitor the network in order to detect intrusions. While both organizations basically fulfill the same purpose and use systems to achieve the same goal, the systems are different (Adams, J., p. 210). This means both organizations pay for the acquisition and maintenance of two different systems that fulfill the same purpose.

The lack of coordination between computer network defense (CND) and computer network attack (CNA) is an additional difficulty of the current decentralized approach to IO that highlights lack of unity and lack of objective. In part, this is due to the way IO currently is integrated throughout the existing force. Revisiting the Air Force structure presented above highlights a good example of this lack of integration. As of February 2001, the AIA has been swallowed-up by ACC. The justification given for this merger was a desire to recognize the role of IO as a war-fighting weapon and bring it into a similar structure as other weapon systems (Air Intelligence, 2000). This approach is not rational when compared with other Air Force organization functions. For instance, ACC originally was intended to be the single source for all air combat weapon systems and associated support and logistic elements. Similarly, Air Mobility Command (AMC) is the single source for airlift weapon systems. From a functional point of view, Air Force

Special Operations Command (AFSOC) and Air Force Material Command (AFMC) exist for the specialties of special operations and acquisition respectively. Therefore, the justification for putting AIA under ACC so that it is treated like other weapon systems is inconsistent when one takes a look at the overall AF structure. In this instance, the AF lacks a clear objective and has put a major provider and conductor of IO under a command that focuses primarily on the dropping of bombs. This is the same as saying IO only has application within actual warfare and nothing to do with the day-to-day operations of the AF. Not only does this not match the AF application of structure and organization, it also could have serious impact on other facets of AF missions other than dropping bombs, such as defense. The DOD approach to defensive and offensive IO also resembles a suspect unity of command and lack of discerning objective. Joint Task Force Computer Network Operations (JTF-CNO) is responsible for clarifying goals for CND and CNA, however, it is subject to the authority and direction of USCINCSPACE. Although JTF-CNO states it operates in conjunction with unified commands, services and DOD agencies (SPACECOM, 2001), the ultimate responsibility lies in the hands of USCINCSPACE. Even though defensive and offensive IO are unified under a single commander, other unified commands are not subject to its authority. This creates an overall disjointed DOD approach to CNA and CND where integration and development occurs in separate commands. IO defense and offense requires a mutual effort from a clearly stated objective not an assumed coordinated effort where the responsible authority is in a separate command. Why is this part of IO so essential?

> Attacks on information systems are already a fact of life in the Information Age…Given our present vulnerabilities as a Nation, a well planned, coordinated IW attack could have "Strategic" consequences. Such an attack or the threat of such an attack, could thwart our foreign policy objectives, degrade military performance, result in significant economic loss, and perhaps even undermine the confidence of our citizens in the Government's ability to protect its citizens and interests. While no "smoking keyboard" has been found to validate such a threat, the very existence of the means to carry out such an attack, when coupled with the myriad of motives and the opportunities that exist, results in our present state of vulnerability. These circumstances have created a situation that calls for prudent defensive actions to be taken in the public interest. We need to be proactive rather than be forced to react after an Information Age "Pearl Harbor." Moreover, a successful strategic attack would point

> the way and encourage others to plan similar attacks. Hence, we need to go on the offense with a vigorous defense. (Alberts, 1996)

The point is that the military must merge its efforts in application of information attacks and information defense. The functional unified command capable of carrying out this task is currently buried in SPACECOM under JTF-CNO that does not operate through an official chain of command.

C. SOLUTIONS FOR CHANGE

Now that we have seen the problems associated with current IO organization: 1) lack in unity of command/no one in charge 2) no clear objective and 3) lack in economy of force/duplication of effort, what solutions can be utilized to bring about appropriate changes in the U.S. military to prevent existing difficulties? The armed forces have attempted to integrate IO into an existing structure. This has occurred at the same time the military states it is in a "Revolution in Military Affairs" due to technology that is a major force enhancer of IO. In order to better facilitate this revolution, we need to consolidate our efforts in approaching IO. Creating a focal point for direction and coordination coupled with the formation of revised policy and formal doctrine is an excellent starting point in the U.S. military's approach to IO. This focal point may be a separate IO command. Basically, the military has tried to force IO into an existing structure as opposed to recognizing IO as a totally new concept and adapting to it in a revolutionary manner. If we develop an IO command, the U.S. military not only follows traditional force structuring, it also has the ability to bring IO services to all ends of the spectrum of application. By having all information experts, from users, gatherers, and maintainers, "under one roof", the military increases its potential for fully exploiting all the prospective advantages that exist within IO. The current structure has this expertise spread out through unrelated areas and treats IO as a weapon only and not as something that has a benefit to how we do business on a day-to-day basis. If we create a new IO command, we will be able to reduce the redundancy of effort and the expenditure of needed funds seen throughout DOD from an IO perspective. Also, the military will be able to combine its efforts in the CND and CNA to formulate a more synergistic strategy

of application. However, before we can combat these problems, one option would be to create a centralized command organization.

D. ORGANIZATIONAL APPROACH

If DOD pursues the creation of a separate IO command, what type of organizational approach should the U.S. military employ to promote the most effective solution? Before an organization can be considered for handling IO, a thorough understanding of the elements of information operations must be understood. At first, the military needs to use the centralized approach it has applied with every major command that emphasizes the strategic apex. The strategic apex of an organization envisioned by Mintzberg plays the most important part in formulation of strategy (1993, p. 14). This type of organization is also one with which the military is most familiar.

This initial beginning will allow the military a chance to establish a central point to formulate clear, concise and effective policy and strategy. There has to be emphasis on definition and applicability of IO. Direct supervision of all major IO players will provide direction and coordination that will allow the new command to take the next step. Once the strategy is formulated, the innovative command can begin its predictable shift to the standardization of work as seen in a machine bureaucracy.

As mentioned earlier, the centralized structure of an emerging IO command does not necessarily have to forfeit the potential paybacks of decentralization. As Mintzberg (1993, p. 98) states, "centralization and decentralization should not be treated as absolutes, but rather as two ends of a continuum." There will be a need for some selective decentralization, "the power over different kinds of decisions rests in different places in the organization" (1993, p. 100), once the new IO command has formulated clear guidance, determined its objectives, and is up and running. Within the fast-paced changes of the information environment, there will be a requirement to shift some power to the analysts, support specialists and operators that Mintzberg describes as " horizontal decentralization" (1993, p. 105). Overall, with respect to the military's approach to IO, we can reap the benefits of both decentralization and centralization.

The Marine Corps' Combat Development Command has developed an extremely comprehensive definition of the elements of IO (Marine Corps CDC, 1998). The elements of IO are depicted in Figure 1 below.

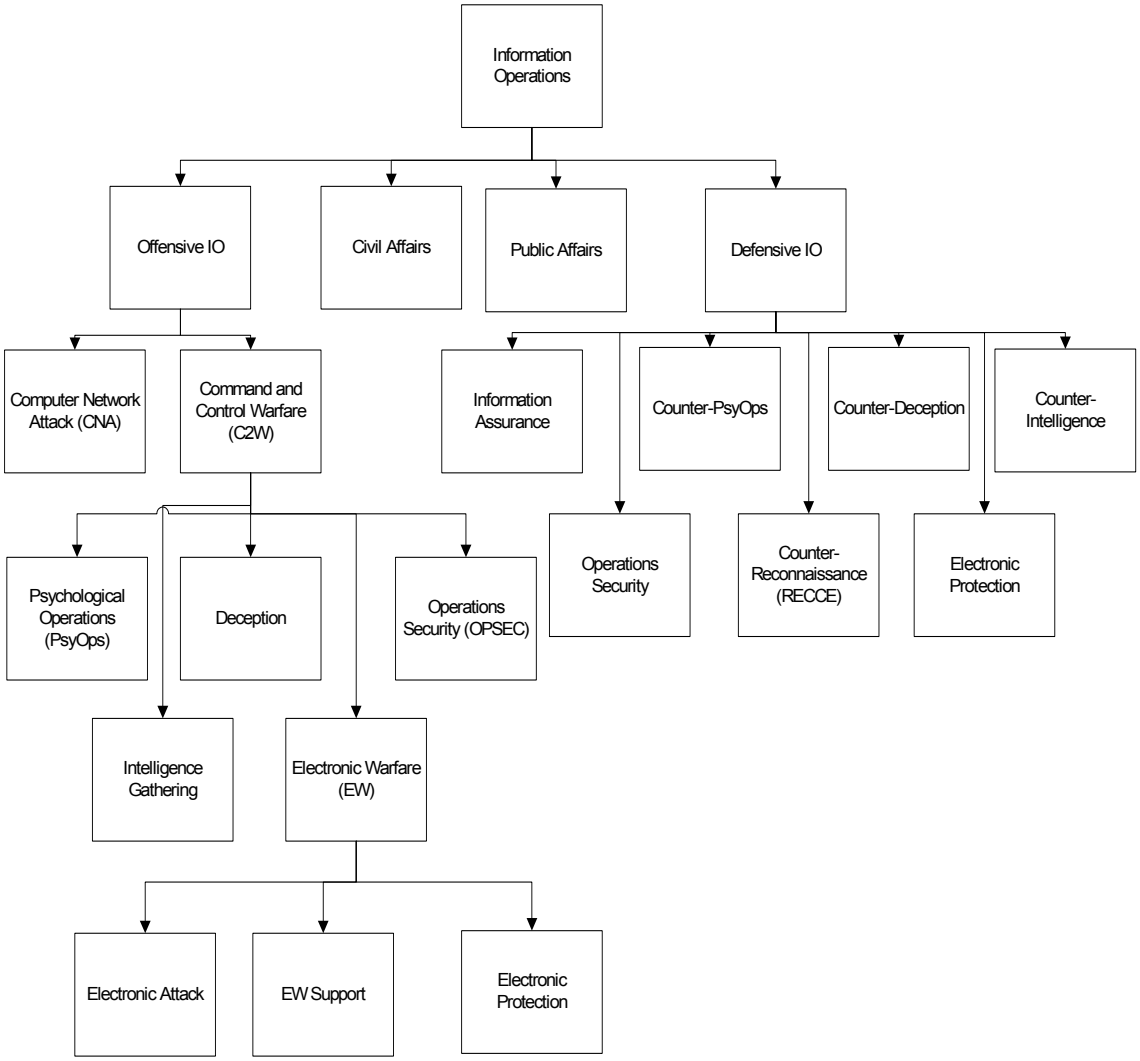

Figure 1. Elements of Marine Corps Information Operations(From: Marine Corps)

As with any aspect of military power, there are both the offensive and defensive realms. As well, both realms are complementary in that offensive actions can neutralize the enemy's ability to attack information systems and thus defend these information systems. Similarly, defensive capabilities ensure the continual ability to launch attacks. Consequently, neither can be conducted in a vacuum. Both must be aware of the actions of the other. The elements of defensive IO are the protection of the information

environment, the ability to detect an attack, the ability to reconstitute after an attack, and finally the ability to respond to an attack. These aspects are typically linked with information warfare and electronic warfare; however, both of these types of warfare are merely subsets of IO.

A complete definition of IO should include any aspect of military operations that involves elements affecting the decision making process with the exception of the application of direct physical force. In that regard, public affairs, civil affairs, psychological operations, and information gathering, i.e., intelligence and reconnaissance, are all elements of IO. Information gathering supports both the successful and accurate application of physical force and the application of offensive and defensive IO. Public affairs, civil affairs, and psychological operations are IO tools necessary for shaping and sculpting the perception of adversaries and allies alike. Thus, these three tools are referred to as perception management tools (Alexander, 1999, p. 111).

Having fleshed out the elements of IO, it is possible to then define IO. IO is the application of tools, methods, or procedures to affect the decision making process of an adversary force while at the same time defending against the ability to affect one's own decision making process. The basis of any decision is information. Therefore, inherent within IO is the gathering and disseminating of information necessary for the decision making process.

The challenge is how to integrate IO within the existing military force in such a manner that allows the ability to utilize IO in daily operations and the ability to capture a corporate synergy from this utilization. The answer to this challenge may be to allocate IO resources under a single command structure that provides IO services to a corporate customer base in such a manner as to not impair the customer's flexibility in its use, yet allow the customer to have a stronger tool that is based on a corporate knowledge.

E. GOALS OF A NEW IO COMMAND

One of the first goals of a new IO command is establishing a focal point for overall direction, coordination, integration and implementation within the IO realm. The current decentralized, ad hoc approach does not allow the effective formation of

applicable doctrine or strategy that is desperately needed to begin addressing IO in the rapidly changing "information age" context. A single entity is needed to bring all facets together to enhance the overall approach to information dominance. Incorporating all IO players (experts, users, gatherers, and maintainers) under a single command will allow the military to exploit all possible advantages of IO and share crucial information essential to an all-encompassing strategy. As the U.S. military struggles to develop IO doctrine in a dispersed way, the enemy continues to improve their ability to wreak havoc in the information domain. Instead of debating IO across the respective DOD spectrum, the U.S. military needs to narrow the debate with a responsible authority as its moderator and as its initiator to begin applying what we know in an integrated way. The military can achieve a solution that is greater than the sum of its parts, but only if it is willing to rethink the manner in which it currently approaches this "revolution". Central control will provide a priceless beginning that will enable the military to establish the course it desperately needs.

Once the U.S. military has reached consensus in an overall IO strategy, then it can begin using some selective decentralization that Mintzberg proposes. The military can still maintain central monitoring for an appropriate response and at the same time delegate responsibility at various levels, but oversight and IO response capability will ultimately lie in the hands of the IO CINC.

From the outset, an additional goal will be evident in the formation of an IO command. As mentioned earlier, a new command will reduce redundancy and duplication of effort with respect to IO. The immediate effects of simply integrating CNA and CND will go a long way in reducing co-existing efforts. We can observe from the examples above how completely separate methodology can arrive at the same conclusions, but not without double the hard work and fiscal expenditures. Our examples cross military service department lines, however, the same efforts are being expended within each branch of service. An IO command will reduce this redundancy from its very inception by centralizing the IO efforts under one roof. The potential cost of centralizing IO is in stifling creativity by having a consolidated organization exploring a new field of study as opposed to having four organizations studying this field. However, this cost can be

greatly minimized by both soliciting input and having the consolidated organization provide IO support to the other four.

Another goal of the new IO command exists where the "rubber meets the road." With regards to the tactical level of operations, individual units should maintain an information operations capability as necessary to complement the overall IO strategy. Marek (2000) sums this point up best when he states,

> As in any military endeavor, it is imperative that all operations at the tactical level support the tactical objectives. These tactical objectives should support the operational strategy, which should achieve the operational objectives. In turn, these should support the theater strategy, which should achieve the military strategic objectives. While tactical operations and objectives may differ markedly from one military unit to the next, they should all support the attainment of the military strategic objectives. In this respect, information warfare is no different from any other form of war-it, too, should seek congruence from the tactical to the strategic level of war. (Marek, 2000)

When the new IO command develops its clear-cut objectives for an overall IO strategy, it will be each unit's responsibility to analyze that strategy and build its own tactical objectives that expand on the new IO strategy. The same processes used at the IO command level will also be seen at the tactical level. How important is the tactical level goal of IO? According to the Army Field Manual 100-6, it is extremely important,

> Information dominance is a temporary tactical condition achievable through a deliberate process. It entails the construction and protection of the information environment, collection of intelligence and relevant information, processing and dissemination of such information, and focused attack against both the enemy's C2 and his eyes and ears. Information dominance facilitates superiority in battlefield visualization at a specific time and place, creating a window of opportunity that is fleeting at best. The commander must seize the opportunity to gain the advantage through effective battle command. (1996)

In preparation for the use of such tactical level IO operations, another goal of the new IO command will ultimately surface. In order for the U.S. military to effectively utilize IO, it should organize and train its forces by efficiently integrating IO into military exercises. DODD S-3600.1 makes this clear,

> Sufficient training, including realistic exercises that simulate peacetime and wartime stresses, shall be conducted to ensure that commanders of US Armed Forces are well-informed about trade-offs among affecting, exploiting, and destroying adversary information systems, as well as the varying capabilities and vulnerabilities of DOD information systems. (1998, as cited in Joint Pub 3-13)

Joint Pub 3-13 also emphasizes that exercises should incorporate IO training from an organizational and individual aspect. It should be clearly put together within the entire process from planning to execution.

Much of the problem in making headway in the area of information defense lies in the fact there is no "smoking gun" (Adams, J., p. 181). This inconceivable train of thought must be turned around if America is to win the wars of the future. It is only a matter of time before the hacker community rises above the military horizon and poses a credible and serious threat to national security. The way to convince the doubters is through exercises such as Eligible Receiver (Adams, J., p. 187). In this exercise, opposing information warfare forces were able to harmfully modify the logistics system used by warplanners to plan and execute war. Such exercises must be implemented within our modern war games. For example, when a major exercise such as Blue Flag, the major air-to-air combat exercise held by the Air Force, is being run, an opposition force should be established to wage information warfare. During Eligible Receiver, the opposition force was able to modify logistic systems so that headlamps were delivered instead of missiles (Adams, J., p. 187). If this were to happen during Blue Flag, surely someone would pay attention. By integrating classified methods of information attack into modern war games, the government can begin to prepare the defense needed to counter attacks against critical systems. As well, the emphasis needed for information operations can be gained by demonstrating that a relatively non-lethal force can be used for dire circumstances.

F. CONCLUSION

The U.S. prides itself in being at the "Tip of the Spear" when it comes to information technology. Even one infamous vice president falsely claimed to have invented the Internet, hence reminding the public how important and prestigious it is to

be at the very top of this technological game in the U.S. With the global proliferation of information comes uncertain consequences that can be catastrophic in relation to future military conflict. From a military perspective, the importance of Information Operations (IO) in terms of protecting vital national interests cannot be overstated. The U.S. must maintain its lead in information technology and systems.

The U.S. military's approach to organizing IO is in direct confrontation with three of the basic principles of war that have been historically successful. Specific examples have been applied to underline this state of affairs. Due to the rapidly changing information environment and previously addressed problems, one solution to DOD's dilemma would be to provide an IO focal point for coordination and direction. It may benefit the military to merge its IO expertise and exploit its "direct supervision" approach it has successfully applied with every major command. Although DOD is currently attempting to use a nontraditional organizational approach by placing IO within an existing structure, it may be appropriate at this time of "Revolution in Military Affairs" to fallback on its historical success with centralized organizational structures. In the past, DOD has stimulated substantial organizational change when it recognized a groundbreaking military concept, thus maintaining its military dominance. If we are going to maintain our information dominance, we must be willing to take the necessary action to move forward. Attempts to find the "smoking gun" in IO may only lead to further delays in establishing a feasible strategy and leave the U.S. unprepared to preempt or counter our information adversaries. When DOD experienced times where the future of warfare was in question, it applied innovative approaches to traditional military structure that promoted unhampered national security. Some cases involved in this recognition and inevitable transformation will be discussed in the next chapter.

III. WHAT CAUSES ORGANIZATIONAL CENTRALIZATION IN DOD?

A. INTRODUCTION

Now that the some reasons why DOD may require an organizational modification with regards to IO have been clarified, understanding what causes organizational centralization in DOD will be beneficial. Using case study research methodology, we can explore possible answers to the title question. This chapter will not provide an in depth analysis of this issue, but an external overview that provides adequate evidence to support the application of a theory that promotes DOD organizational centralization of information operations. By analyzing several historical cases, this research offers evidence concerning why creating a separate information operations organization may be appropriate at this time.

In the context of this study, organizational centralization is a change in any DOD organization where that organization becomes its own centralized, separate command. A centralized military organization is important, because it is critical to its effective operation within the current structure of DOD and to carrying out its desired goals. Without a centralized organization any military force can become overwhelmed by countless goals, objectives and strategic concepts that can encourage the failure of that organization over time. Some nations no longer exist today due to inadequate military organization. Effective military organization is critical to the defense of a country against its enemies (national security). National security applies across the spectrum; in other words it is crucial to all nations who want to maintain their independence in the world and keep their nation's culture, norms, and values unscathed from outside influence. In order to preserve their independence and success as a nation, they must be successful at any venture to include military conflict, akin to being a successful world power.

B. SELECTED CASES AND WHY

We will use the following cases in order to examine organizational centralization in DOD: INDENT 1), 2), 3), 4), TO .5

1) Formation of the USAF as a separate service.

2) Establishment of USSOCOM.

3) Current progress in creation of NORTHCOM following 9/11.

4) Air Corps following World War I.

We use these specific cases because they are all classic cases where the U.S. experienced recognized and vital losses during military conflict. In history, the U.S. has been active in the success and independence of its own values, norms and culture. From the definitions of variables below, it is evident that each case contains some variation and aspect of the variables that should be included in this research.

First, the U.S. military needed to reorganize following WWII because they wanted to remain a successful world power. Although the U.S. did not experience substantial air power failure during WWII, its allies did. This highlighted its need to adjust its military organization, improve its technological advantage within a changing external environment, and provide funds in pursuit of an air superiority advantage.

Second, the U.S. military also needed to reorganize following several failures including the Iranian hostage rescue attempt and the Grenada operation. Again an external threat was evident. The rise of a new kind of war doctrine promoting low intensity conflict increased this threat.

Third, the most recent example of failure for the U.S. is 9/11. This significant loss propelled DOD into action by organizing a new Unified Command-NORTHCOM. This case is unique because it occurred very rapidly relative to the other cases. It is important to observe this case because the U.S. can make changes to organizational structure when needed.

Lastly, the Air Corps case provided is a control case to make a plausibility probe into the other cases examined. It provides a look at a case where the military did not experience recognized failure and assumed it did not have an external threat change that threatened its success as a nation. It is used to strengthen the theory addressed by the other cases.

C. INDEPENDENT VARIABLES

Organizational centralization can be the result of several variables. The variables utilized in this research include: 1) recognized, possible failure in conflict, 2) no clear chain of command, 3) change in external threat, 4) innovative product champion, and 5) the inability to effectively apply military force.

One cause of organizational centralization within DOD is a recognized, possible failure in conflict, which means for the purposes of this research, a large or unreasonable loss of lives that is publicly identified and spurs fundamental change in military doctrine. Failure forces a nation to take a close look at why it happened. It seems this investigation is only natural given a world that puts so much emphasis on success and independence. If a nation is not successful in military conflict, they must answer why and attempt to correct the mistakes so it will not happen again to maintain their own separate culture. The resulting correction in doctrine normally gives birth to force structure and organization modification. By itself, failure may not necessarily mean a nation will form a centralized military structure. However, failure in concert with other variables does give rise to organizational centralization.

One such factor that helps stimulate a centralized military configuration in combination with failure is the lack of an explicit chain of command. For the purposes of this research, a clear chain of command is one that provides a command structure with an unambiguous decision-making process. When a nation fails in conflict, it must explore why and adjust or fine-tune its approach to conflict to avoid future failures. Its first step in this course of action is ascertaining "who is responsible" or "who is in charge". This cannot be truer in the U.S. Our culture educates us from birth to go straight to the person in charge. This kind of attitude already exudes a tendency to promote a search for the pinnacle of a centralized group. The U.S. private and public sectors usually know exactly who the "belly-button" is and where the ultimate responsibility lies. Therefore, in order to adjust any organizational makeup to prevent future failures, we normally start at the top and then work our way down. The military's answer to this kind of adjustment involves a centralized organizational structure.

Another cause of centralized military organization within DOD occurs from changes in the external threat. In order to preserve national success and independence, as triumph in war accomplishes, nations must be prepared to thwart threats from external environment alterations. In this research, external threat changes are advancement in technology and/or other nations' actions that promote a superior military force. This advancement creates fear of dwindling national success and independence in other nations. From this fear, undue pressure arises for the nation without advancement to amend its methods to overcome external threats, which reduce that nation's ability to uphold its success and independence. These amendments in harmony with other variables create a need for centralized military organization.

An innovative product champion has also prompted organizational centralization in DOD, in part. In this research, a product champion is someone who has the ability to look into the future and promote a somewhat drastic change to existing military organization to ensure U.S. national security. With today's emphasis on military innovation, it seems we have reconciled that this is a prominent factor in the future of warfare. However, before now, our innovative activists encountered insurmountable road blocks, where at times he had to be willing to sacrifice his career to make the appropriate changes needed. This research shows that product champions were recognized in response to military failure and external threat to modify or sometimes revolutionize outdated thinking in order to uphold our national security. It seems the military is really serious in its pursuit of innovative thinking, but normally they wait until the environment is sufficient to support change.

One other variable that will be discussed in this research is the inability to effectively apply military force. Even though at times, this variable helps incite organizational centralization, but it does not occur in all cases. Therefore, it is not defined or operationalized in this summary.

In Table 1 below, the resulting independent variables for each case evaluated are summarized. It illustrates, from the analysis of each case, the variables that were at work that facilitated the centralization of that organization within DOD.

Independent Variable	USAF	USSOCOM	NORTH-COM	Air Corps after WWI	IO Command
No Clear Chain of Command		X	X		X
Innovative Product Champion	X	X		X	
Possible Failure In Conflict	X	X	X		X
External Threat	X	X	X		X
Inability To Apply Force		X			

Table 1. Independent Variables

D. ANALYSIS—USAF

Carl Builder's account of the birth of military aviation and organization of the U.S. Air Force is very thorough (Builder, 1994). His in-depth look at the history of the Air Force demonstrates the aspects of recognized failure, external threat and product champions which provoked the establishment of a centralized Air Force organization.

Prior to WWII and following Pearl Harbor, the War Department underwent several changes that promoted centralization for many organizations. This well-known disappointment along with the recognition of possible collapse of democratic nations helped prompt an overall look at the War Department's ability to sustain national security. The reorganization of the War Department in 1942 gave the Air Corps a degree of autonomy second only to independence.

> Further recognition of the status of the air arm came in July 1943 when the War Department stated its official position in Field Manual 100-20, *Command and Employment of Air Power*: "Land power and air power are co-equal and interdependent; neither is an auxiliary to the other." (Goldberg, 1957, p. 100)

External technological improvements all over the world produced by a rapidly paced industrial revolution fueled new theories of warfare. Times were changing at an increased rate. The speed of information and air travel drastically increased, thus external threats became evident, and a new kind of war ensued. This new kind of war no longer existed in the realms of theory; it now staked its claim in reality. Recognized possible failure coupled with an external threat promoted a centralization of DOD organizations to include a separate aviation organization.

> ...military aviation had opened up a completely new and dominant dimension of warfare-not just an adjunct to surface warfare-which could produce quick and decisive results in war if exploited through offensive strikes directly at the critical sources of enemy power; but to do those things, military aviation must first be used to control the air and be centrally and independently controlled. (1994, p. 62)

According to Builder, air power offered a unique ability to strike at the heart of the enemy (1994, p. 62). Air power could obtain the primary objective in war—victory. It could stop the enemy's will to fight by turning the enemy's population into a terrified, nonsupporting mass and destroy the enemy's command centers and production capability. "Air power wasn't just a new means for waging war, it could be seen as the most effective means for getting directly to the central objective of war" (1994, p. 60). The War Department (DOD) recognized the future threat of military aviation. Along with this threat, it realized that failures were not only possible, but absolute.

Following WWI, various product champions arose to promote the theory of military air power, which at this time was paramount in the prosecution of a centralized aviation organization. Although some of these air power prophets dated back to WWI, their ideas were carried forward to a time when external threat and recognized failure were more prevalent. It is clear that the three most prominent air power theorists had consistent influence on each other.

Giulio Douhet, Hugh Trenchard and Billy Mitchell were the first air power pioneers to address the organization of military aviation. Although Douhet's ideas were not all his own, he was the first to write them down and they were, "the most coherent, the most systematic and the most prophetic air power writings of the era" (1994, p. 50).

Douhet used graphic descriptions of air power's use on civilians. When air power was used on this "sustainer of war", it would provide quick victory that would spare lives. His founding principle stated that, "to conquer the command of the air means victory; to be beaten in the air means defeat and acceptance of whatever terms the enemy may be pleased to impose" (1994, p. 60). He added that, "in order to assure an adequate national defense, it is necessary—and sufficient—to be in a position in case of war to conquer the command of the air" (1994, p. 60). Consequently, to accomplish all of the above hypotheses, Douhet said the Air Force must be independent. During WWI, other air power pioneers encountered the psychological effects of German aviation. The British had first-hand experience with the strategic bombardment from German Zepplins, which had traumatized the British homeland. Hugh Trenchard, commander of the Royal Air Corps recognized how to exploit the moral influence of the airplane on an enemy in a strategic air offensive method to deter significant losses during WWI trenches and attacks on British territory. Trenchard believed the best way to handle the air arm in WWI was to

> …unify all aviation under one commander, to place the minimum number of airplanes necessary for the use of ground troops in action with each army, and to concentrate the bulk of bombardment and pursuit so that he could hurl a mass of aviation at any one locality needing attack. (1994, p. 52)

Although Mitchell promoted his plans in a different way, his thinking was in line with Trenchard and Douhet in that, "his actions were to reserve as much as possible of the air power available to the Americans in a single strike force for the offensive" (1994, p. 52). He also said, "in order to unite and bring your greatest effect to bear in any one place it is necessary to unite all elements of your aviation at one place where the decision is called for..." (1994, p. 61).

All three of these air power activists identified the need for an independent Air Force where the decisions could be made in one place, in other words organizationally centralized. As a champion, Mitchell's dedication to the pursuit of air power theory cost him a court-martial and eventually his career in order to promote the ideas that would one day become Air Force doctrine, but he laid the groundwork for further sponsorship. His selfless sacrifice and devotion to service paved the way for many other air power

advocates that would recognize the same roadblocks, but in time would establish the Air Force as a separate service.

Although there were numerous innovative advocates of air power, it would take years for the U.S. to take military aviation seriously. The U.S. did not suffer the losses their Allies encountered in the Great War and they had the Atlantic Ocean as a buffer. However, the growth of technology allowed the external threat to become more realistic and new air power advocates entered the scene: 1) New precision bombing techniques developed at America's own Air Corps Tactical School showed strategic bombardment could be pinpointed and 2) Two new supporters, Henry "Hap" Arnold and Ira Eaker explained that air travel would make the Atlantic and Pacific Oceans look like the Mediterranean. Hap Arnold utilized a different approach than Billy Mitchell. He was dedicated to the Air Force as an institution to promote independence and a large bomber force without trampling those in his way. He had a good reputation in Congress and in the public. Strategic bombardment technology and Arnold's political prowess led to President Roosevelt's endorsement of long range bombing before the start of WWII. Arnold's thoughts concerning a centralized organization were evident when he said,

> The task of the military airman now departs from a crusading role. It becomes a task of organization on a tremendous scale. No longer do we require flaming leaders with fanatic zeal to sell a cause; we need sound, even-tempered minds of great resource and depth to perfect the plans and build the structure of an air force larger than the armies and navies of old. (1994, p. 102)

Even though the U.S. was in the middle of a depression, Roosevelt increased the budget for the Air Corps and made more money available through the Public Works Administration, "expressly to buy airplanes and inject life into a dying aircraft industry" (Nalty, 1997, p. 136). From this point forward, a separate Air Force was only a matter of time. Arnold became Deputy Chief of Staff (For Air) in 1939. During WWII, numerous congressmen introduced bills for an independent Air Force based on studies of the subject and public opinion. Finally, President Truman signed the National Security Act of 1947, which established the U.S. Air Force as a separate organization. In the aftermath of Pearl Harbor and in the face of future failure in conflict, increased external

threat, and with formidable proponents of air power, the U.S. was able to secure its future by creating a centralized Air Force.

The creation of a separate Air Force can be used as an appropriate model needed to qualify the current IO organizational dilemma in DOD. Several factors described in the Air Force are inherent in IO as well. First of all, the degree to which IO will play in prospective military operations is unquestionable for the U.S. as well as other nations or small groups—it will be paramount. Hence, an external threat exists. Second, like the beginnings of air power, IO will offer its users an innate ability to strike at the central objective of its enemy and provides a new way of conducting warfare. DOD should, like the past War Department, recognize the future threat of IO and realize that possible failures can occur. Addressing the need of an innovative product champion, DOD should transfer this impetus to relative Air Force inception time periods. Although Mitchell and other air pioneers clearly stated their concerns that would ultimately affect air power doctrine, it was not until Arnold's political techniques surfaced that the Air Force made actual progress toward separation. In other words, the air power advocate issue was mainly separate from the question of organizational centralization. The chief thrust of centralization came from the external threat and possible failure in this new kind of warfare. Albeit, DOD should "do as they say" and carry out the innovative thinking it so often stresses. When the time is suitable, it should become the product champion for new IO doctrine.

E. ANALYSIS—USSOCOM

Susan Marquis' description of the creation of USSOCOM is very detailed and provides another good example of the formation of a centralized organization due to recognized failure, no clear command structure, external threat, product champions and the inability to apply effective military force.

As with the formation of a separate Air Force, recognized failure of the botched Iranian rescue attempt and needless loss in the Grenada operation was the final straw in the quest for a separate U.S. Special Operations Command. Prior to these events, Special Operations (Spec Ops) had proven its worth in WWII and the Korean War. "When the tensions that highlighted a need for special operations forces relaxed, however, the new

Special Forces group lost much of its support" (Marquis, p. 12). Following Desert One, it was clear that something had to be done in order to preserve American military dominance. Marquis describes the aftermath the best when she said,

> Iranian television footage of the burned bodies of U.S. servicemen and their aircraft in the Iranian desert horrified U.S. citizens and encouraged an international perception of U.S. impotence before a handful of Iranian students and a new revolutionary government. (Marquis, p. 3)

Three years later, another Spec Ops failure would come to light during Congressional hearings that, "revealed the Grenada operation was badly mismanaged and may have involved unnecessary loss of life" (Adams, T., p. 193). U.S. limits in the unconventional domain were now internationally exposed. The recognition and public awareness of these failures magnified the importance of finding a solution to the U.S. Spec Ops problem. One answer was to properly organize Spec Ops to prevent bad decision-making and mismanagement.

In the wake of such failure, the search was on to find out who was responsible. While U.S. air power had fallen under Army as it rose in significance, Spec Ops control was sprawling and diluted over all the military services, thus spreading out responsibility so no one was ultimately in charge. Conventional leadership wisdom as a result of the "Fulda Gap" war, endorsed the doctrine of overwhelming the enemy with unlimited power, holding ground and confronting the enemy in direct conflict. Therefore, any leadership attempt to promote clandestine operations, sabotage, and ambushes was seen as irrelevant and un-American. Marquis describes the status of Spec Ops forces within the U.S. military as one with "precarious values" (1997, p. 7). "Precarious values are those goals or missions within an organization that are in conflict with, or in danger of being overwhelmed by, the primary goals or missions of the organization" (Marquis, p. 7). Each service had its own perception of Spec Ops and in addition, thinkers whose primary motives were conventional warfare drew up the goals and objectives for these service-unique Spec Ops forces. With this fractured management and direct resistance to its principles, Spec Ops had no identified responsible authority or command structure. Recognized failure, partly as a result of this lack of a clear chain of command, propelled the U.S. toward a more centralized approach to Spec Ops.

With rising tension in Vietnam and following another recognized failure in the Bay of Pigs, President Kennedy expressed his thoughts concerning Spec Ops,

> This is another type of war, new in its intensity, ancient in its origins-war by guerrillas, subversives, insurgents, assassins; war by ambush instead of combat; by infiltration, instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him...It requires in those situations where we encounter it...a whole new strategy, a wholly different kind of force, and therefore a new and wholly different kind of military training. (Marquis, p. 13)

Mao Tse Dong and Ho Chi Minh identified a new, unconventional variant of warfare that offered the U.S. a viable external threat. However, conventional leadership opposition and nonsupport within Kennedy's own staff caused widespread misuse of Spec Ops as they were conventionalized. In other words, Spec Ops forces were unable to effectively apply their military potency against this new kind of war, because military leadership used their unconventional talents in a conventional way. This abuse clarifies the need for a separate Spec Ops command structure to make unconventional decisions at one place. A fractured Spec Ops status remained intact following the Vietnam conflict, because once again the need for Spec Ops had deteriorated as the U.S. began to concentrate on the Cold War. The result of Spec Ops' inability to appropriately apply its new kind of warfare as identified by an external threat and its lack of a centralized decision-making authority was the inevitable failures it experienced. To solve this seemingly overwhelming problem, U.S. Spec Ops needed an all-encompassing answer that a separate command may provide.

Although well-publicized failures fueled the start of the centralization of Spec Ops, the most prominent factor in the formation of USSOCOM was the success of its product champions. General Edward Meyer was one of the first to recommend a separate Spec Ops organization. "He thought the United States could not afford to ignore the rest of the world while focusing on the Soviet threat" (Marquis, p. 62). After becoming the Chief of Staff of the Army and following Desert One,

> he proposed a new combatant command called Strategic Services Command (STRATSERCOM), whose mission would be to counter terrorism in peacetime or in periods of conflict short of war, and to protect

> the U.S. leadership and command and control centers in a major war with the Soviet Union. (Marquis, p. 73).

Even though he recognized the military's dedication to a potential WWIII, the response to his proposal was nonexistent. "All the services feared STRATSERCOM as a fifth Service, feared it would take away their responsibilities and cut into their resources" (Marquis, p. 73). It seems senior military leadership was more worried about resources and responsibility than preservation of national security. The seesaw battle of Spec Ops utilization was now motivated by an all-out unconventional war within the very bowels of DOD itself. Noel Koch, Lynn Rylander and Colonel George McGovern became Spec Ops strongest promoters. As Marquis describes, Koch, a principal deputy in the Office of the Secretary of Defense (OSD), had a strong interest in counterterrorism. McGovern became his military assistant and "he had a strong network all over the building (Pentagon), all over the country, and all over the world" (Marquis, p. 80). When Rylander joined their fight, he had numerous contacts within DOD and he was a "fervent believer in the value of special operations forces and the need to look outside Central Europe for the most immediate threat to American national security interests" (Marquis, p. 80). Like Billy Mitchell, each of these advocates was willing to sacrifice his time, career, and even life to advance U.S. military dominance. When McGovern died in 1982, Koch was more determined than ever to build a Spec Ops Command. While Koch spearheaded efforts within OSD, Rylander attacked Spec Ops foes in the Pentagon. Koch created a Special Planning Directorate streamlining his authority to the SECDEF and put together the Special Operations Policy Advisory Group of retired, Spec Ops experienced general officers who outflanked Spec Ops opponents and put pressure on the SECDEF from the outside. The result was a SECDEF-directed policy statement written by Koch and Rylander that ignited a JCS proposal to look at, "how best to organize to provide the CINCs with the best special operations capability" (Marquis, p. 85). From this point, Koch shifted his tactics to a more public forum. With gaining support in Congress, Koch increasingly highlighted the weakness of Spec Ops. In 1984, Senator Strom Thurmond read one of Koch's speeches into the Congressional Record. In 1986, House and Senate appropriation committees directed DOD to report on, "the feasibility of creating a single command structure for special operations" (Marquis, p. 130). Senators William Cohen

and Sam Nunn also entered the public debate recognizing the applicability of Spec Ops in aftermath of Desert One, Grenada and increasing terrorist actions. Together, their influence on Spec Ops would become law in November 1986. The Cohen-Nunn legislation established U.S. Special Operations Command (USSOCOM), formalized Spec Ops activities, and created Spec Ops funding separate from other services. If not for the commitment of these supporters, Spec Ops would have continued its seesaw battle for recognition.

The U.S. military's misuse and inability to efficiently utilize Spec Ops forces and its inadequate decision-making structure gave birth to internationally distinguished failures. These failures coupled with the increasing external threat of terrorism and military operations other than war and with innovative advocates who realized Spec Ops significance enabled a centralized USSOCOM to become reality.

There are several points to emphasize in the formation of USSOCOM that are relevant to possible IO organization. The USSOCOM case highlights several innovative supporters. However, as in the Air Force case, the reasoning behind their existence is separate from the issue of organizational centralization. In effect, the champions' influence was substantial, but their efforts were the result of competition with conventional leadership resistance. In the SOCOM case, unlike the Air Force case, failures in conflict occurred. DOD has yet to experience any IO failure, but that does not indicate that it will not. In the analysis of the Grenada failure, mishandled operations may have caused unneeded casualties. Is DOD going continue an argument of ignorance and wait until they incur unnecessary IO related deaths before the organizational pitfalls of current IO policy are modified? In DOD's inspection of Spec Ops control, it found that ultimate responsibility was unknown and command guidelines were immeasurable. As discussed in the previous chapter, this also characterizes the current structure for IO. While IO may not be the object of resistance that Spec Ops was prior to SOCOM, it does lack a clear chain of command. Also, like Spec Ops, each DOD organization, agency or individual service component maintains its own IO perception, since they have not come into contact with it before. Allowing separate IO opinions may encourage misuse of IO assets and permit primary organization objectives to overpower any IO benefit. Because IO guidelines are not centrally specified and because DOD lacks any sort of "Fulda Gap"

wisdom for IO, it makes it even more imperative to understand that this is a radically new kind of war. Like unconventional warfare, IO requires a completely new strategy and a different kind of military force. A new IO command may provide the responsible authority DOD needs to develop successful, cohesive IO doctrine.

F. ANALYSIS—NORTHCOM

With the recent events of 9/11 fresh on the minds of the world and the U.S. government, a new strategy seems to be solidifying. Secretary of Defense, Donald Rumsfeld answered why this is happening,

> Current events should teach Americans the peril of the unexpected. We have to recognize that it is not possible to know every conceivable threat that can be posed against our country, friends, allies or deployed forces. We have to recognize the kinds of capabilities that exist and deal with those capabilities wherever they happen to come from. (Garamone, February 2002)

Not only has this publicly recognized failure prompted quick action from the Department of Defense, but ever-growing external threats of possible second attacks and increased international terrorism has spurred another adjustment to the Unified Command Plan. According to DefenseLINK, DOD has released details of a new Unified Command Plan that includes the establishment of U.S. Northern Command (Garamone, April 2002). This new command structure will generate a military, "that is better equipped to defend the homeland from terrorist attacks...and create Northern Command that would be responsible for defending the borders, coasts and airspace of the United States" (Lerman, 2002). Here, DOD has also identified that it does not contain the proper structure, which allows an understandable chain of command. Overall, DOD has prepared plans to establish another separate, centralized command structure in light of a well-known failure, recognized and unidentified external threats and a lack of a clear command structure for making appropriate and suitable decisions.

9/11 is a case that closely resembles why a new IO command may be pertinent at this time. NORTHCOM demonstrates DOD's ability to establish a suitable chain of command where it is nonexistent. When it comes to U.S. military dominance and preservation of national security, DOD can react very quickly. Although DOD has not

experienced an "electronic" 9/11, it has identified potential IO failures. The SECDEF is also very clear about recognizing and dealing with external threats. Is DOD going to remain in reaction-mode only or are they going to preempt the death toll experience of 9/11? Like NORTHCOM, a new IO command may be able to formulated a comprehensive plan that will preclude loss of international status and retain national security.

G. ANALYSIS—AIR CORPS FOLLOWING WWI

Following WWI, recognized failure and external threat for the United States were difficult to imagine. Its entry into the Great War had prompted victory for the Allies. The U.S. did not recognize the reality of "gut-wrenching" trench warfare, because these conflicts were not fought on their own soil. The Atlantic and Pacific Oceans stood between the U.S. and any external threat that an enemy might impose.

Even though a centralized Air Corps did have its outspoken activists, they were considered "cowboys" that would not be recognized until WWII. Not only were these first air power prophets disregarded, but an established War Department organization was difficult to fight. At that time, the War Department was pleased to fall in line with isolationist's ideals. The buffer provided by large bodies of water alone offered the protection of American culture needed to preserve its independence. There was also an adequate command structure where the Air Corps remained under Army ground control. When necessary, the Air Corps could provide essential ground support for the kind of war of that day.

Overall, although there were several critics, the War Department did not see an external threat or failure following WWI, and the Air Corps was well established in the most successful warfare doctrine of the time, therefore no centralization of the Air Corps occurred.

H. CONCLUSION—INFORMATION OPERATIONS (IO) COMMAND

The U.S. takes great pride in being on the "leading edge" of information technology. This means the U.S. military not only requires a technological information advantage, but it needs to be unsurpassed in its readiness and capability for IO in order to protect itself from all enemies. "The mission of DOD is to provide the military forces

needed to deter war and to protect the security of the United States. Nothing less is acceptable to us, or to the American people" (DOD, 2001). The cases above can be used, as appropriate models required for qualifying the current IO organizational dilemma in DOD. Factors described in each case are essential in IO as well. With the advent of the "Information Age" and the proposition of a fundamentally new kind of war, military operations involving IO is undeniable. "The scale and pace of recent change have made traditional means of defining future military operations inadequate" (TRADOC, 1995). Presently, there is a major push for innovative thinking in DOD and the U.S. military. However, is the military really serious in its pursuit of innovative thinking or do we have to wait until the environment is sufficient to support change? As seen in the preceding examples, groundbreaking thinkers influenced the future doctrine once a centralized organization was born, but although they were present, their concerns were not what ultimately caused organizational centralization. Only when the time was right (i.e., failure in conflict and external threat) did their ideas rise in validity. With these innovative supporters aside, it does seem that DOD may be killing valuable time in pursuit of a valid information operations (IO) plan. Currently, like Spec Ops before USSOCOM, IO is spread out over individual services and DOD agencies resulting in broken management with no clear "belly-button". In order to resolve this problem, one option is to utilize the future-thinking methods that DOD considers so vitally essential. So far, IO activists are buried in separate organizations; however, that does not indicate the time for change is not right. With that said and if feasible, DOD's innovative mindset has an opportunity to provide centralized IO command that will allow the formation of IO specific goals and a clear line of responsibility. NORTHCOM is a good example of how DOD can make fitting changes if desired. As with NORTHCOM, not only does DOD have an external threat and possible or realized failure, IO has no clear chain of authority. No IO baseline exists and fractured responsibility can lead to inconsistent goals that can be overwhelmed by primary goals of decentralized units. As in unconventional warfare, IO requires a new kind of strategy with an accompanying military organization.

From the cases above, there seems to be enough evidence to determine an IO Command may be appropriate at this time. There is an external threat and although there has been no noteworthy IO failure, there are recognized IO failure theories. Also from

the above illustrations, DOD has suffered significant failures unrelated to IO. It knows failures can and do happen and cannot plead ignorance. This realization should be enough to seriously consider a radical change in current IO structure. Does DOD have to wait until there is an "electronic" Pearl Harbor or 9/11 or can DOD learn from its mistakes? In the wake of 9/11, NORTHCOM has appeared to centralize the decision-making and force employment capabilities of the U.S. to prevent attacks on U.S. soil. Presently, there are continuing debates if this type of 9/11 action will spill over into the IO domain. What are some examples of IO external threat and possible failures? DOD should consider how China dramatically stepped up its cyber attacks on the U.S. following the P-3 incident and how U.S. hackers declared war on Arab countries following 9/11. Also, take the recent California power troubles for instance; although this was not the product of information based attack, imagine if it was the result of enemy direct action. Consider the consequences of an attack that resulted in long-lasting electricity blackouts in metropolitan areas where critical hospital care was closed down. Other examples of IO threats could be frozen bank accounts and ATMs from virus-corrupted bank systems, or oil and gas sabotage in the middle of winter. Our country will survive, but some of us may not. These cases may not be as catastrophic as 9/11, but how many lost lives are too many? It will still be a failure that infringes on our culture and freedom we enjoy. "Are we going to a world where freedom is allowed to flourish" (Garamone, February 2002)? Or will it be a world where electronic terrorism spreads from country to country until we are at the will of the information tyrants (Garamone, February 2002). The U.S. holds the future of information operations in its hands. Historically, DOD has waited until it was too late to save precious lives. If it begins with a centralized organization where the responsibility, planning and objectives can be determined, it may prevent needless suffering and promote the freedom it cherishes. A new IO command may provide the responsible authority DOD needs to develop successful, cohesive IO doctrine.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. AN INFORMATION OPERATIONS ORGANIZATIONAL STRUCTURE MODEL

A. INTRODUCTION

Having examined what causes organizational centralization in DOD, it is now necessary to examine what a centralized structure for providing IO services to the CINCs and individual services would look like. To that end, this chapter describes a generic organizational structure for providing IO services in the military environment. It is generic in that it is not tied to an individual service, i.e., Army, Air Force, or Navy, and it is not tied to any of the existing unified commands. The goal of the organizational structure described here is to provide the same services that are provided in the current military and, at the same time, provide increased capability that is realized through the centralization of efforts and resources. The contention is that the centralization of the intellectual capital associated with IO will result in higher returns that can be seamlessly integrated throughout the DOD or any service via a single command that reaches into all aspects of the DOD or any service. Finally, the model is intended to be applicable within the individual services or at the unified command level.

B. TERMS

The organizational structure used in this chapter is intended to be generic with regard to the branch of service or level of DOD to which it is applied. In that regard, generic terms have been used to describe the various levels of any particular branch. In order to assist with understanding the generic terms, an application of these terms in reference to the Air Force's organizational structure is depicted in Figure 2. The figure assumes corporate support is being provided to the AF. The AF major command ACC is provided divisional support. Unit or location support would be provided to a Special Tactics Squadron (STS) or Langley AFB, respectively. Hopefully this will aid the reader in understanding the levels of command that are implied with the words corporate, divisional, and unit or location.

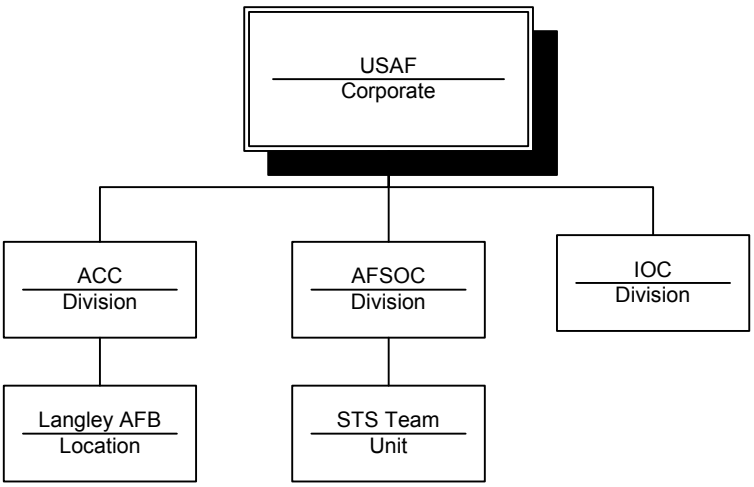

Figure 2. Application of Terms

C. THE STRUCTURE

An organizational structure for implementing a consolidated approach to IO that meets the needs of individual units is depicted in Figure 3. At the strategic apex (Mintzberg, 1993, p. 13) is the commander of the IO command. The support staff and technostructure needed to support the commander and the command comprise legal, future concepts, commercial interface, and public affairs. Legal and public affairs would compose the support staff (Mintzberg, 1993, p. 16). Future concepts and commercial interface would compose the technostructure and would seek to standardize doctrine, tools, and methodology throughout the command and corporate service (Mintzberg, 1993, p. 15). The middle line comprises corporate support, divisional support, unit and location support, operations, and product development and distribution (Mintzberg, 1993, p. 14). Divisional liaisons are formalized positions to facilitate coordination between the command level and the customers at the divisional level (Mintzberg, 1993, p. 92). Each of the individual areas are described and expounded upon in the following sections.

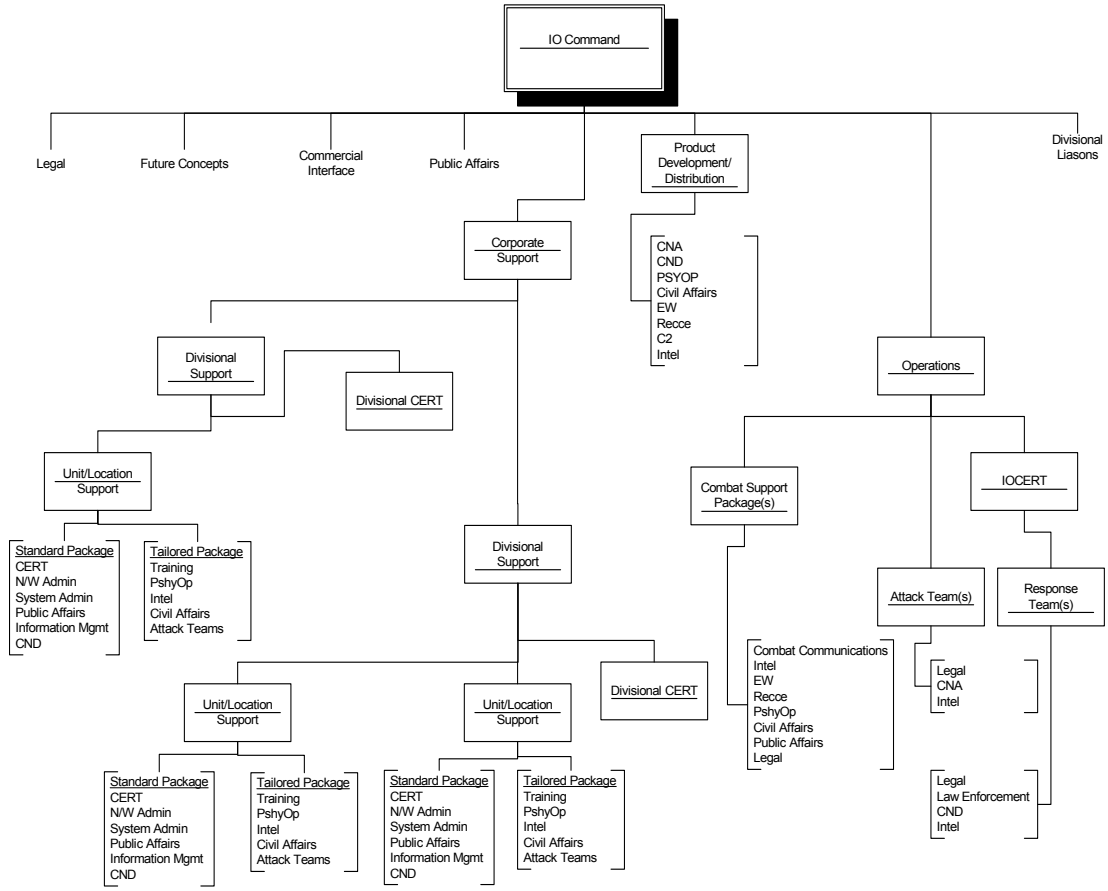

Figure 3. IO Command Structure

D. LEGAL

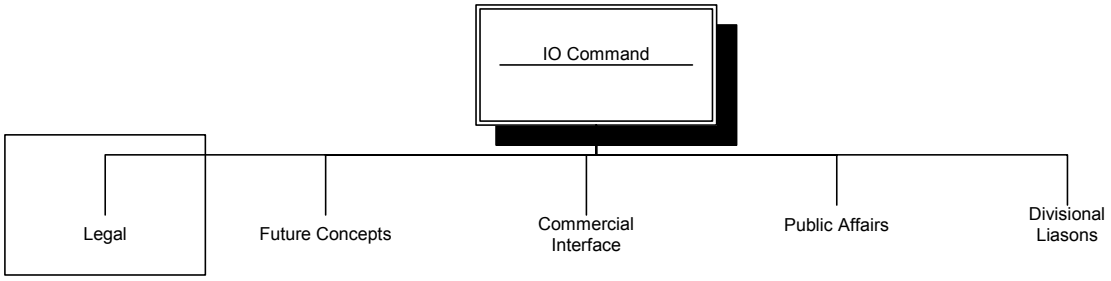

Figure 4. Legal

With the advent of the Internet and globalization, information sharing and privacy have become major concerns. In addition, federal law places boundaries on the involvement of the military in domestic matters. The design of new network attack tools and the defensive capability of tracking automated attacks dictates the need for legal professionals skilled in the areas of individual privacy and *posse comitatus*. Such a function in the support staff, as depicted in Figure 4, would be able to create sufficient

expertise in these areas that does not currently exist. As an example, when hackers attack individual units, the legal ramifications of tracking the hacker and the means of tracking often require a legal review (Adams, 1998, p. 194). This places an unnecessary delay in the process of responding to hacker attacks. As well, when IO attacks are needed against an adversary, the legal ramifications of the attack in regards to international law must be clearly presented to a combatant commander.

E. FUTURE CONCEPTS

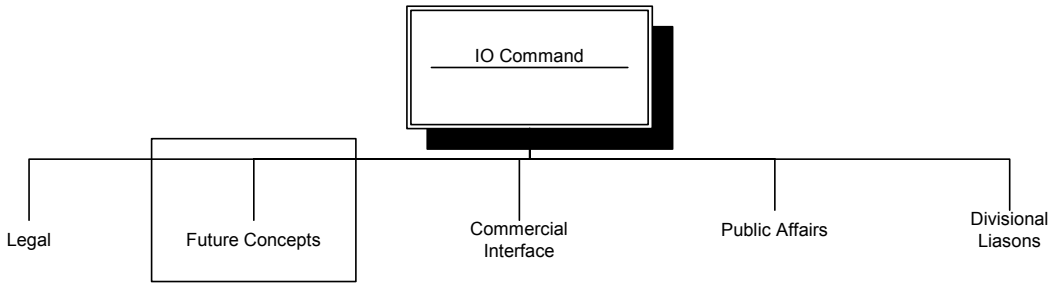

Figure 5. Future Concepts

According to many people, the military as a whole is currently in a revolution in military affairs based on the advancement and implementation of technology (Adams, 1998, p. 56). In order for an IO command to maintain pace with advancements in technology, a future concepts function, as depicted in Figure 5, will be needed at the IO command level. Such a function would allow a single repository for advanced concepts in the realm of IO and would eliminate redundant efforts and expenditure of funds across other military commands. A potential model for the make up of this function would be the battle lab concept implemented in the Air Force. These labs were created in diverse areas to develop innovative new ideas and the implementation of these ideas in the existing force (Battlelabs, 2001).

F. COMMERCIAL INTERFACE

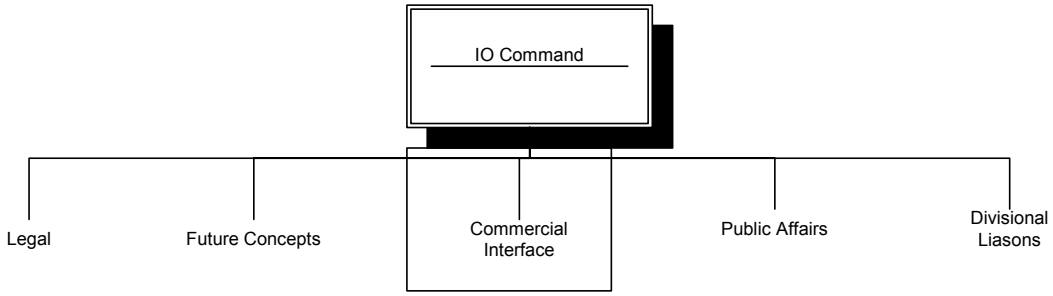

Figure 6. Commercial Interface

Historically, the military was the driving force in technology research and development. This is no longer the case today. Currently the commercial sector is driving the advances in technology (Adams, 1998, p. 57). Indeed, the military's current struggle is to take commercially developed products and implement them in the military environment. A commercial interface, as depicted in Figure 6, working closely with future concepts, would potentially be able to drive commercial industry to develop products that could be more easily integrated in daily military IO. As well, such a function would be an enabler for new levels of cooperation between the military and civilian sectors in regards to defensive information operations. The lines between military and civilian communication systems and areas of strategic interest, i.e., power grids, financial systems, etc., is blurry at best. Both sectors could greatly benefit from a partnership that facilitates information, technique, and idea sharing.

G. PUBLIC AFFAIRS

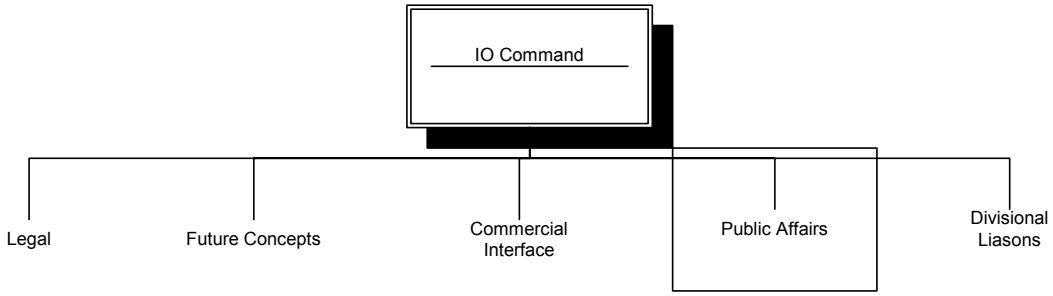

Figure 7. Public Affairs

Public opinion has a major impact on any military operation and indeed the day-to-day existence of the military (Marine Corps CDC, 1998). The opinion of the taxpayer is of vital interest to the success of the military. As an example, when casualties were incurred during the Beirut bombing of the Marine barracks and during operations in Somalia, the perception of a negative public opinion caused the respective administrations to terminate these operations. The relaying of information to the public is a function of public affairs. Similarly, perception management, attempting to control the perception of a respective audience, is a function of IO. Therefore, the placing of public affairs, as depicted in Figure 7, in the IO command would facilitate managing the perception of the civilian sector, which is of vital interest to the military. Ideally, this function would serve as the single point of public affairs for a particular branch of the

military. This would enable all public affairs officers to "sing from the same sheet of music".

H. PRODUCT DEVELOPMENT/DISTRIBUTION

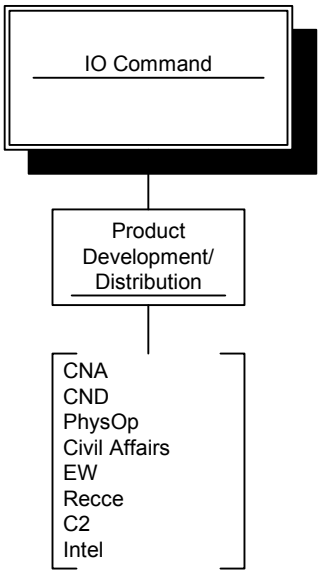

Figure 8. Product Development/Distribution

Currently, there is little in the way of a consolidated approach to the development and distribution of IO related products and systems. In order to accomplish this consolidation at a corporate or branch level, a product development and distribution function, as depicted in Figure 8, would need to be established within the IO command. This office would work closely with the future concepts and commercial interface offices to ensure compatibility of and the ability to integrate new products throughout the service. As well, this function would work closely with an acquisition division at the corporate level.

By placing this function within the IO command, new products could be seamlessly distributed throughout the organization, as needed, down to the individual unit or location. Figure 9 depicts the interrelation between the future concepts, the commercial interface, and the product development/distribution functions.

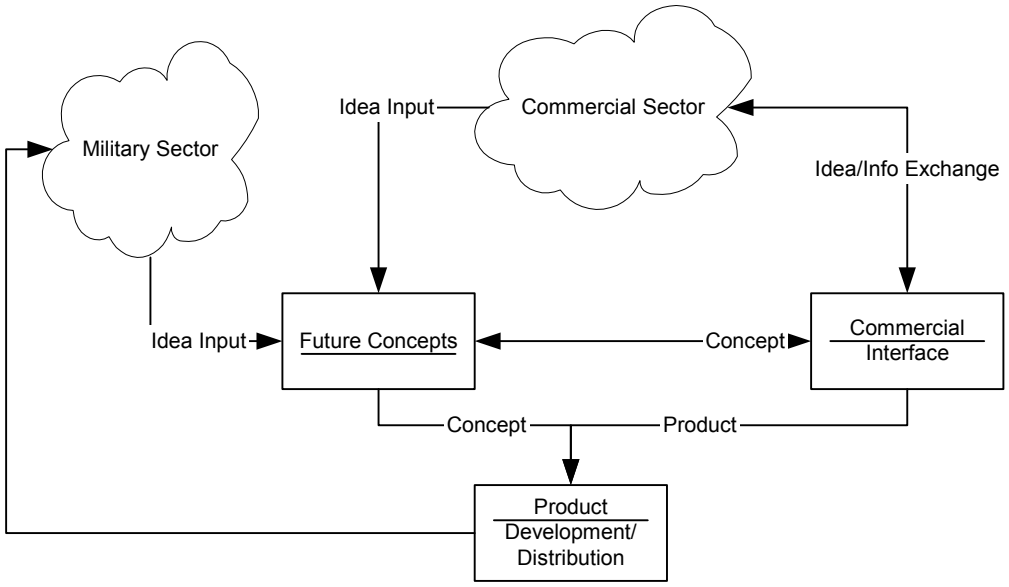

Figure 9. Interrelation Diagram

I. CORPORATE SUPPORT

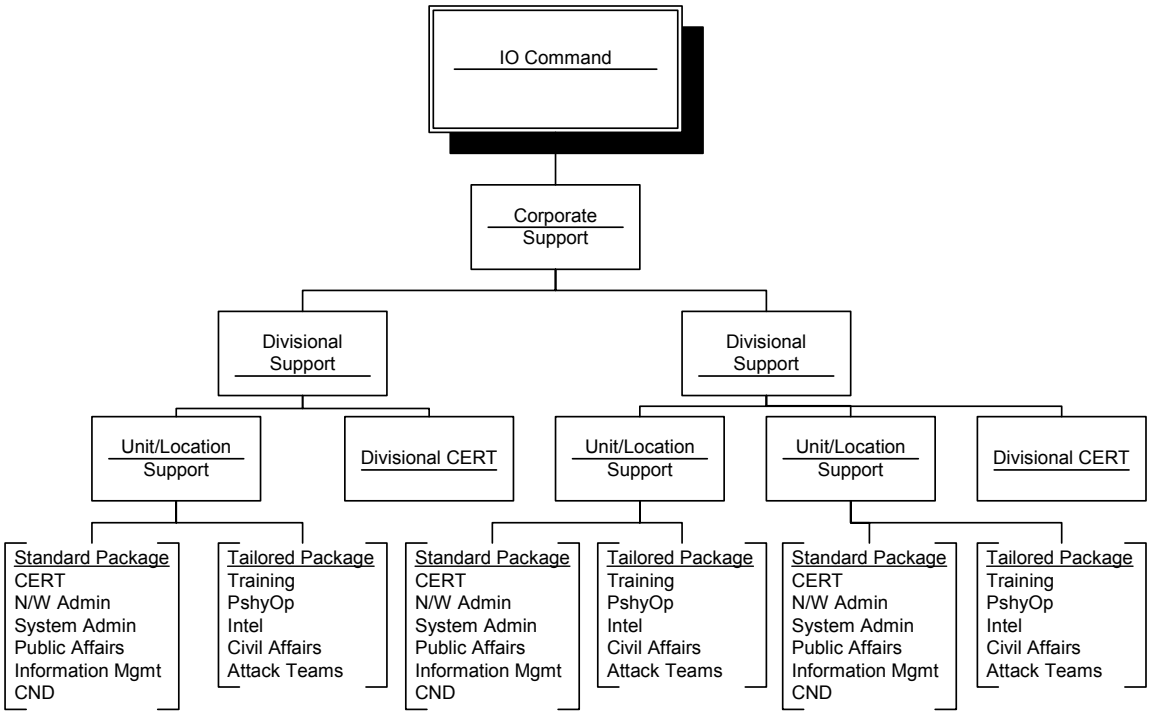

Figure 10. Corporate Support

Each branch of the military is divided into divisions, i.e., MAJCOMS, that support a specific function or mission. Case in point is the topic of this paper, an IO command, or division in the generic sense, which will support the specific function of IO.

As well, these divisions have subordinate bases or units. These divisions and respective units would become the customer base for the IO command. In order to meet the needs of these customers, a formal organization to provide divisional support, such as the one depicted in Figure 10, would need to be established within the IO command. A divisional IO commander would report formally through the chain of command to the IO commander, but would meet the requirements of the branch divisional commander, or customer, in a matrix form. Similarly, the unit/location IO commander would report formally to the division IO commander, but would meet the requirements of the branch unit/location commander who reports to the branch divisional commander. To ensure that the respective IO commanders maintain focus on the customer in this matrix, divisional liaisons at the divisional office level will facilitate requirements, problems, etc. between the IO commander and the divisional commander. The combination of a matrix association and the liaison position is intended to keep the natural inward focus of a large bureaucracy, which could be the result of creating the IOC, in check. Figure 11 shows the flows of formal and informal authority and communication.

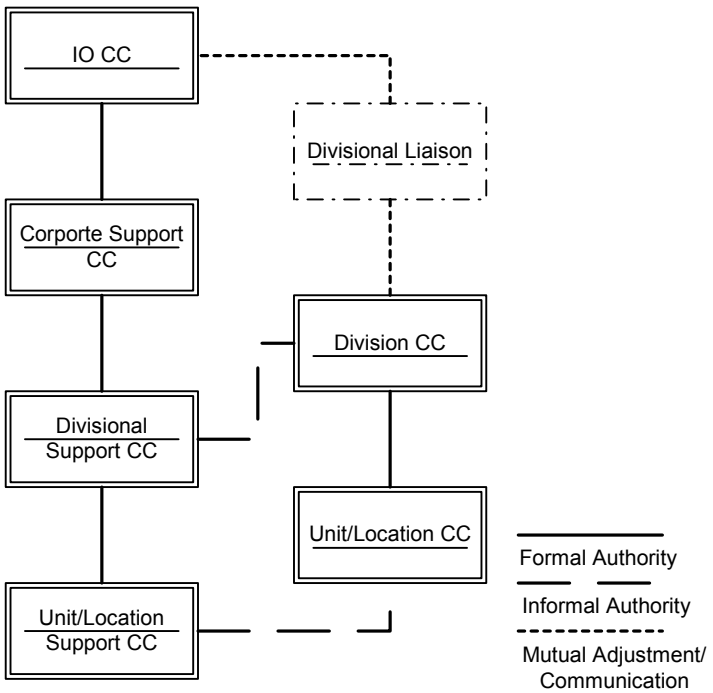

Figure 11. Flow of Authority/Communication

At each IO divisional support level would be a computer emergency response team (CERT). A CERT would also exist at each IO unit/location support level. The purpose of these teams would be monitoring the network for intrusions or attacks. This is a similar model to what is being done in the Navy and AF today (Adams, 1998). Both divisional and unit CERTs would funnel information to the IO CERT, which would fulfill the corporate, or branch, responsibility for network monitoring. The CERTs at the various levels would work together via formal and informal communication to cooperatively ensure the integrity of military data networks. An IO CERT and divisional CERT are needed to provide big picture views of network attacks. As an example, this hierarchical approach would be necessary to detect a consolidated effort to attack numerous sites within the military organization. Figure 12 shows the process and communication flow for the CERT establishment.

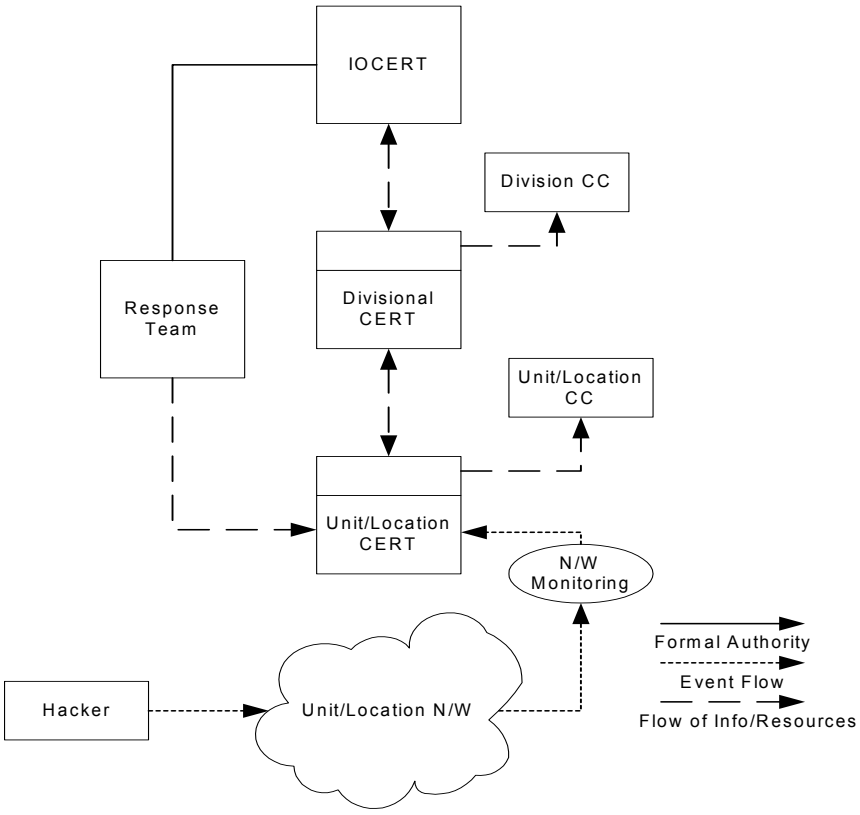

Figure 12. CERT Process

In the case of dedicated attack effort, a response team would be dispatched to the specific unit/location to handle the attack.

At each unit or location two IO support packages could be implemented. The standard package would be implemented across the board as it contains the necessary functions for daily operations during times of peace and war. The functions of the tailored package could be implemented at each unit or location as the mission of that unit or location dictates. For example, a special operations unit would need self contained attack teams in order to mesh with small teams or forces typically used in a special operations environment. As well, specialties regarding training could be integrated throughout a training division or implemented in unique areas, such as special operations. While these tailored functions would be integrated with the customer's environment, they would still report through the IO command structure. Such an arrangement would allow the most flexibility to the customer while still allowing IO resources to take advantage of corporate knowledge and information.

J. OPERATIONS

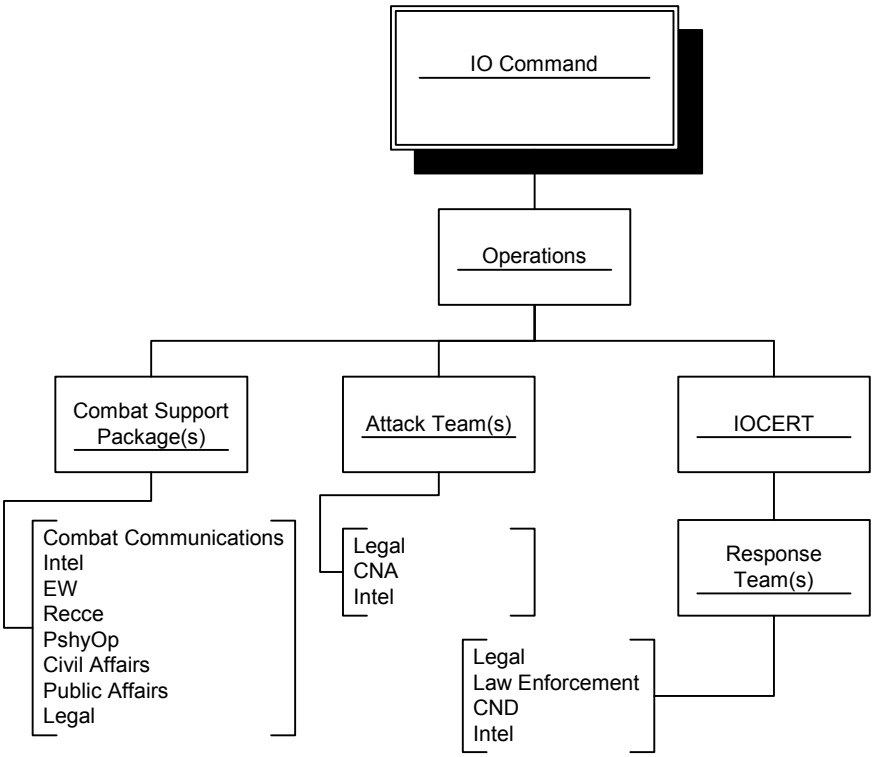

Figure 13. Operations

The IO command would need the capability to provide operational support to all corporate areas during both time of peace and war. The operations function of the IO command, depicted in Figure 13, would facilitate this function. This organization would

be divided into three areas: combat support packages, attack teams, and the IO CERT with its associated response teams.

The first area, combat support packages, would consist of a go-to-war capability needed to support a combatant CINC in any theater. The number of packages could be determined by regional constraints, i.e., one for CENTCOM, EUCOM, PACOM, etc., or could be constrained by doctrine such as the ability to fight two simultaneous major regional conflicts. A combat support package would provide a combatant commander with all the realms of IO needed to prosecute a war. As well, it would provide the combatant commander with a single point of contact, the combat support package commander, for all IO related issues. As an example, a JTF commander currently has a J6 that serves as the single point of contact for all communications requirements in support of the JTF's mission. Under this concept, this JTF commander would have a J-n, the combat support package commander that handles all IO related issues. While this in effect is a centralization of functions to a single individual, it is also a decentralization of authority for currently separate tasks from the JTF commander to a single individual. During times of peace, the combat support packages would be integrated with combat units during exercises. This would not only increase combat effectiveness, but would also facilitate the realization of the capabilities of IO as a combat enhancer. A combatant commander who loses his combat capability due to the implementation of an IO attack will have a greater appreciation of IO, and it is better that this happen during a peacetime exercise as opposed to during actual combat. Finally, a combat support package would also include a response and attack team who would report to the combat support package commander for the duration of the exercise or war.

The second area is attack teams that would comprise expertise in legal issues, computer network attack, and intelligence. Legal would be included for the same reasons already discussed regarding the legal function on the IO command staff. Intelligence personnel would be required for determining desired target and effect. The computer network attack personnel would be needed to facilitate the actual attack. Intelligence and computer network attack personnel would work together to assess the effects of the attack. The attack team is not integrated into the combat support package, because the combat support package is a major conflict response. There may be times when an attack

team is needed when a major conflict is not occurring. Finally, some attack teams may be integrated with actual units due to the specialty of the unit's mission, as discussed in the corporate support section.

The final area, the IO CERT, would fulfill the purposes already discussed in the description of the divisional section. The response teams would be tasked by the IO CERT during peacetime and would be aligned in a matrix manner to the combat support package commander during times of war. Legal, law enforcement, computer network defense, and intelligence personnel would comprise the response team. Law enforcement and legal would work together to determine the means used in responding to the attack, i.e., the feasibility of a counter attack, tracking methods, etc. Intelligence personnel would gather data on the nature, origin, and method of the attack. As well, intelligence personnel would gather any data available on the human source of the attack. The computer network defense personnel would repel, terminate, or allow, for the purpose of gathering intelligence, the attack. If a counter attack is deemed legal and prudent, members from an attack team would augment the response team or an attack team would be dispatched to join the response team.

K. CONCLUSION

This chapter has described a centralized organizational structure for providing IO related functions in the DOD. The attempt has been made to ensure the proposed structure provides for all aspects of IO. As well, the structure attempts, through integration with the larger organization, to realize the gains that can be realized from centralization without leaving the larger organization bereft of the services the structure provides due to the inherent inward focus of large centralized, bureaucratic organizations. Components of the structure, i.e., Future Concepts, aid in realizing the benefits of pooling the intellectual capability associated with IO. Similarly, components such as Corporate Support and Divisional Liaisons work to ensure the proposed organizational structure remains responsive to the larger organization as a whole.

V. AN APPLICATION OF THE MODEL

A. INTRODUCTION

Having looked at the generic model for creating an organizational structure necessary for efficiently implementing IO, the natural question occurs of what would this model look like in actual implementation? To answer this question, we will look at implementing an IO organization at the unified command level. For any such organization to be feasible, it must use existing organizations in new ways. Due to the fiscal constraints of today's defense budget, DOD cannot afford to build organizations, no matter how badly needed, from the ground up. Keeping this principle in mind, this paper attempts to present a unified command for IO, appropriately called the United States Information Operations Command (USIOC). Figure 14 depicts an organizational structure for the USIOC.

The currently existing elements necessary to create such a command are determined by the description of an IO cell within a Joint Task Force (JTF) (Joint Pub 3-13, 1998). The rest of this chapter is spent discussing the elements of the structure in detail.

B. LEGAL

Research does not reveal any single joint or service associated legal body specializing in the realm of IO. Therefore, the USIOC would have to develop this legal expertise. The areas of knowledge would relate to the legalities of launching and responding to computer network attacks, implementation of psychological operations internationally, and general military law, i.e., Law of Armed Conflict. This "pool" of knowledge would consist of enough personnel to support the operational assets of the unified command, advise the commander and other staff, and interface with other governmental legal bodies, i.e., FBI, Attorney General, etc. Since this capability does not currently exist, the USIOC would potentially have to develop or support some form of schoolhouse necessary for growing the desired talent.

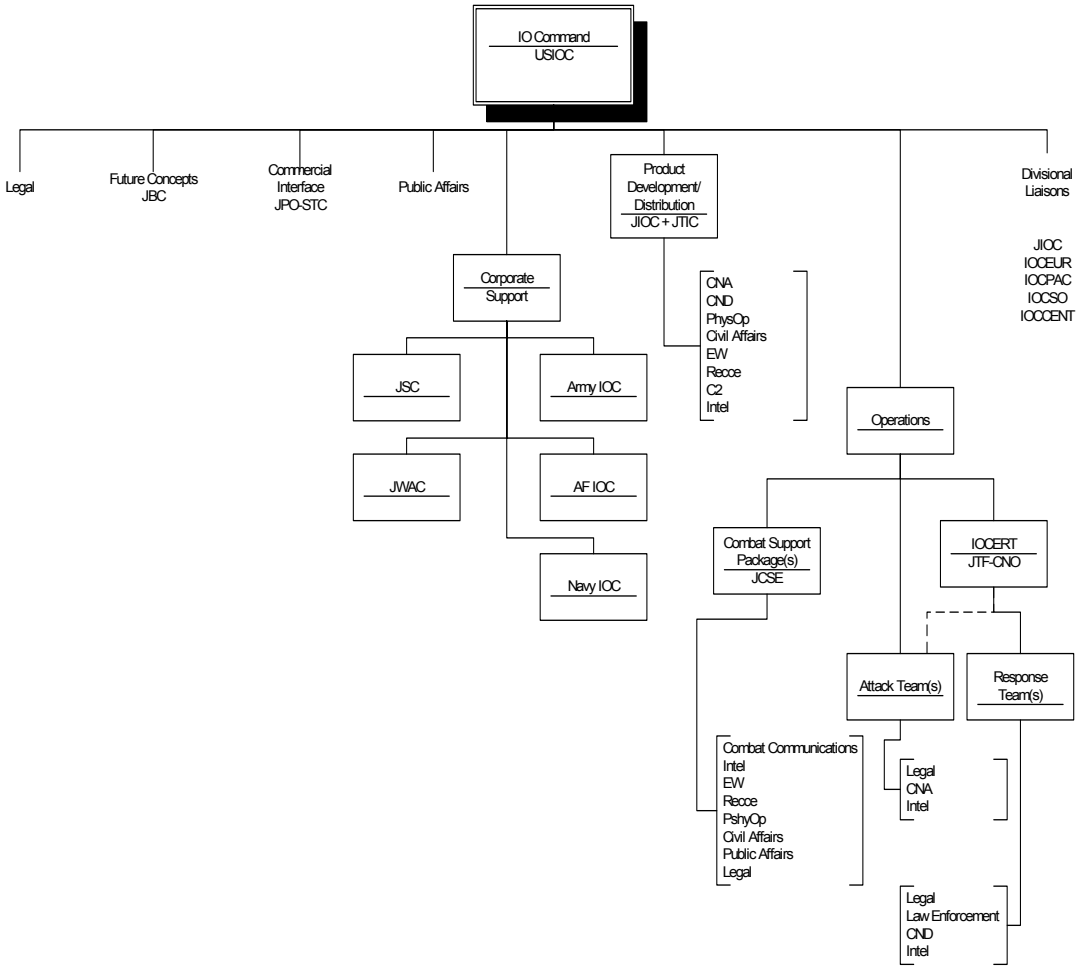

Figure 14. USIOC

C. FUTURE CONCEPTS

The purpose of Future Concepts is to develop new and innovative means of performing IO related functions in the future. Currently, the Joint Battle Center (JBC), under United States Joint Forces Command, is best poised to perform this function. The JBC currently performs technology assessments of Command, Control, Communications, and Computers; Intelligence; surveillance; and Reconnaissance (C4ISR) capabilities (JBC Mission Brief). The focus of these assessments is to identify and recommend technologies that are needed to support warfighter's needs in the JTF. This capability provides the foundation needed to enable the experimentation and assessment required for a Future Concepts function within the USIOC. The only change that would need to

be made to the existing organization would be expanding the C4ISR capabilities with the other elements of IO, i.e., Psychological Operations (PSYOP), Civil Affairs (CA), Electronic Warfare (EW), etc. By combining all these various elements into a single arena, i.e., Future Concepts, the visions of interoperability and collaboration become exponentially more achievable.

D. COMMERCIAL INTERFACE

Commercial Interface is the component of the command that works with commercial industry to both keep abreast of the latest advancements in technology and to ensure telecommunication assets essential to DOD operations are kept secure and available. The candidate organization that exists today to fulfill this requirement is the Joint Program Office – Special Technology Countermeasures (JPO-STC). The purpose of this program is to:

> … provide DOD decision-makers, Commanders-in-Chief (CINCs), and operational commanders with an analysis and assessment capability to identify critical infrastructure susceptibilities and operational dependencies that, if not assured, could adversely impact mission accomplishment of military operations vital to national security. (JPO-STC Brochure).

While this program does get into areas that are not directly related to IO, i.e., railroad systems, electric power, etc., it does include the areas essential to IO, i.e., telecommunications, intelligence, surveillance, reconnaissance, etc. As well, the additional areas relate to information needed by operational units and commanders, and this information represents what an IO command exist to provide, i.e., information superiority. The only area that would need to be increased within JPO-STC is the focus on taking advantage of technological advancements in commercial industry. This function would involve identifying key technologies and best practices utilized in industry. Any key technologies could be feed to the future concepts function of the USIOC. This would keep the two working together such that industry could feed the military, and the military could help identify threats to industry and ensure necessary safeguards are in place.

E. PUBLIC AFFAIRS (PA)

Research does not indicate there is any joint or otherwise consolidated organization that supports the public affairs function within DOD such that there is a singleness of message. The creation of a USIOC and its subordinate service level commands would create this ability. Within the realm of IO, PA is a critical capability in the area of perception management. This capability is needed to garner public support for military operations and to combat disinformation campaigns launched by enemy forces. By creating this proposed structure for PA, the capability to train and educate PA officers and staff to facilitate perception management will exist. With proper training, PA officers would be able to advise commanders on how the message should be portrayed as much as what the message should say. This will provide CINCs, and the DOD as a whole, with a greater capability than the mere ability to serve as an information conduit that exists today. Under the USIOC concept, USIOC would become the PA force provider for all DOD.

F. CORPORATE SUPPORT

Corporate Support comprises organizations that would support the sister unified commands of the USIOC and the DOD as a whole. This area would be under the command of a single individual within the USIOC. The areas that make up the Corporate Support that provide support to all sister commands and the DOD are the Joint Spectrum Center and the Joint Warfare Analysis Center. The areas that provide support to the individual services are the component commands: Army Information Operations Command (AIOC), Air Force Information Operations Command (AFIOC), and the Navy Information Operations Command (NIOC). These last commands are commands that would need to be created as subordinate commands to the USIOC, similar to the way the component special operation commands are subordinate to the United States Special Operations Command (SOCOM).

1. Joint Spectrum Center (JSC)

In essence, the JSC ensures the availability of the frequency spectrum the DOD needs to allow seamless communications that are free of interference (JSC Mission). Also included under the responsibilities of JSC are the information assurance aspects of

information warfare as they apply to the spectrum dominance. This capability would exist under the USIOC to facilitate supporting the C4ISR requirements of the JTC. No additions or changes would need to be made to this agency, other than putting it under the command of the USIOC to facilitate relaying information to the component IO commands that are the JFC's force providers. In short, putting JSC under the USIOC is merely the process of aligning related functional support to functional force provision.

2. Joint Warfare Analysis Center (JWAC)

JWAC provides infrastructure analysis to CINCs for the purpose of directing force application. This organization examines the civilian and military capabilities associated with a potential adversary from an infrastructure point of view. As a provider of information critical to a warfighting CINC, this organization would fall under Corporate Support within the USIOC. The advantage of placing JWAC under the control of the USIOC is found in the parts of the puzzle that JWAC does not currently provide. Under the umbrella of effects-based operations, being under the USIOC would increase the JWAC's capabilities. While JWAC looks at the physical, it does not look at the psychological, nor does it map network attack capabilities. By combining PSYOP personnel with the capability of JWAC, it now becomes possible to provide a CINC with potential targets and the effect that neutralizing those targets has on the decision-maker's will to continue the fight. Add CA to the equation as well, and it becomes possible to determine the effect force application, to specific targets, has on the continued working of an enemy's government. As well, by combining network attack personnel with the capability of JWAC, the CINC has some middle ground in terms of physically destroying a target or just making the target inoperable. To further add to the benefits from such an organization, the combatant CINC's operational plans could flow through the enhanced JWAC for the purpose of developing the initial shell of a war plan or for the development of detailed regional plans. By placing JWAC under the USIOC, it is possible for a single force provider to provide a list of targets and the effect of taking those targets out to a warfighting CINC.

3. Service Components

As stated earlier, each service would stand up a service component, similar to the way USSOCOM has the US Army Special Operations Command, the Air Force

Operations Command, and the Navy Special Warfare Command, that would be subordinate to the USIOC. It is beyond the scope of this paper to describe these service components in detail, but a rough idea of the makeup of each is given here.

The AIOC would be comprised of, at least, the Land Information Warfare Activity (LIWA), the 11th Signal Brigade, and the US Army Civil Affairs and Psychological Operations Command (USACAPOC). USACAPOC would be the lead service organization for satisfying the civil affairs and psychological operations manning requirements of USIOC. In order to fully integrate these capabilities throughout the broad area controlled by the USIOC, manning levels within USACAPOC would probably have to be increased.

The AFIOC would be comprised of, at least, the Air Intelligence Agency, the combat communications assets within the Air Force (AF), the Air Force Communications Agency, the Information Warfare Battle Lab, reconnaissance and surveillance flying assets, and any psychological operations assets within the AF. The combinations of these assets would enable the creation of combat support packages, within the AF, that could provide a deployed wing commander the entire C4ISR package.

The NIOC would be comprised of, at least, the Navy's new information technology command and the Navy Component Task Force-Computer Network Defense (NCTF-CND). With just a quick glance at the Navy, this command would be relatively small, as there does not seem to be a clear method of separating the Navy's C4ISR functions from aboard ship. However, creation of such a command could greatly facilitate the ability to push critical information to the "floating" war. As well, the creation of attack teams would provide a shore-based asset for the sailing naval warfighter.

G. PRODUCT DEVELOPMENT/DISTRIBUTION

Combining the Joint Information Operations Center (JIOC) and the Joint Interoperability Test Command (JITC) would create Product Development and Distribution. These two organizations have the unique skill sets that would be needed to create a single DOD source for the rapid development and deployment of C4ISR related systems and policy. The implication of this capability is the USIOC, similar to

USSOCOM, would have the acquisition authority necessary for awarding contracts and the associated program management authority necessary for system development.

The JIOC provides support to operational commanders by integrating operational security, PSYOP, military deception, electronic warfare, and destruction (Kreighbaum, 1998). JIOC also plays a role in the development of joint doctrine, tactics, techniques, and procedures in the aforementioned areas. These capabilities combined with the ability to integrate various command and control database to form a common joint information base, make JIOC the prime candidate to develop IO related products and procedures and ensure distribution of these capabilities to the unified commands and individual services. The only change that would need to be made to JIOC would be a greater focus on the CNA and CND arenas as well as removing the requirement for JIOC to have deployable assets to assist combatant commanders. These deployable assets would be integrated with the operations side of the USIOC organization. Furthermore, this would allow JIOC greater ability to focus on the developmental side of IO without the worry of meeting or maintaining an unknown operational tempo.

To complete the product development and distribution organization, the JITC would have to be added. The JITC, which currently belongs to the Defense Information Systems Agency (DISA), performs interoperability testing on C4I and combat support systems (JITC Mission/Vision, 2001). This capability would be essential to any product development and distribution function within the USIOC. As new systems are developed, their interoperability with existing systems could be determined by the JITC. By combining JITC with JIOC, interoperability testing can begin with system development and be an integral process as opposed to a final hurdle for system development that could potentially delay or stop system release. At the unified command level, this capability could also be used to ensure service level systems are interoperable with other service systems and with joint systems, by either mirroring this capability as the subordinate component level or requiring all system development efforts to work closely with the USIOC. Currently, the DOD lacks a joint development activity to overcome the interoperability hurdle. While joint program offices do exist, they usually exist with a particular service being named the lead for the program. Human nature dictates that a service lead agency will always have the concerns of its mother service

foremost on its mind. Under the USIOC, joint systems could be developed and disseminated in a truly joint environment.

H. OPERATIONS

The USIOC, as a supporting unified command, would require an operational capability to support the needs of the combatant commands during times of hostility. Within the USIOC, a single individual would be designated in charge of all operational assets within the USIOC. These assets would consist of one or more combat support packages with the number being determined by either national objectives, i.e., the ability to maintain two major regional conflicts simultaneously, or by maintaining one to support each regional commander. Since each service component of the USIOC would maintain a deployable capability as well, the first rule would probably be the most feasible for determining the number of combat support packages needed. As well as combat support packages, there would need to be an Information Operations Computer Emergency Response Team (IOCERT) to ensure the capability is maintained to monitor DOD networks during times of hostility and peace. Finally, the capability to have deployable CNA teams under the operations function would be needed to perform automated attacks. The reason for having deployable teams is that access to a specific enemy's networks may only be possible by physical presence at a specific node within the enemy's network. An example would be any country that is not directly connected to the Global Information Infrastructure, a.k.a., the Internet; currently, Iraq is not connected to the Internet due to United Nations sanctions.

1. Combat Support Package(s)

The core for the combat support package would be the Joint Communications Support Element (JCSE) (C4ISR Handbook). JCSE is an elite communications unit that has the capability to support two JFCs and two Joint Special Operations Task Force (JSOTF) commanders. With its ability to deploy in 24 hours, JCSE is an ideal candidate for providing the core of any combat support package. In order to be fully viable under the concept of the USIOC, the elements of intelligence, electronic warfare, reconnaissance, PSYOP, CA, PA, and legal would have to be added. Some of these elements would come from JIOC's current deployable assets. If the need dictated, CNA teams could be added to the package as well. From an IOCERT point of view,

monitoring the deployed networks could be handled from the IOCERT itself without needing to deploy any assets. This integrated capability would give a JFC or JSOTF commander a single staff element responsibly for all C4ISR capabilities. These commanders would no longer need to worry about the needs of a J2, intelligence, and the needs of a J6, communications, as separate issues because they would all be rolled into one under the combat support package approach. To further increase the capability of the combat support package and the usability to the combatant CINC, the package, or packages, would be able to tailor to meet the specific needs of the combatant CINC. For example, if the CINC only needed a PSYOP capability, only those assets would be sent to support the CINC. Also, under the USIOC, the combat support package could deploy with information developed by the enhanced JWAC, which increases the ability to apply rapid effects-based operations, assuming the CINC has the operational assets required in place. Finally, the combat support capability directly under the control of the USIOC would primarily be used for scenarios that require quick reaction.

2. Information Operations Computer Emergency Response Team (IOCERT)

The IOCERT exists today, but it is not used or placed in the logical or unified manner needed to be the most effective. The Joint Task Force – Computer Network Operations (JTF-CNO) is tasked to provide the defense of all DOD networks and, when called upon, to perform CNA activities (JTF-CNO Fact Sheet, 2001). Currently this JTF is aligned under the US Space Command (USSPACECOM), a supporting command. Aligned under USSPACECOM, the automated aspects of IO, i.e., CNA and CND, are separated from the non-automated aspects of IO, i.e., PSYOP, CA, etc. This results in CNA and CND operating in a vacuum and disjoint from the capability to field an integrated and unified IO capability to the combatant commands. Under the USIOC, this capability would be under the same "roof" as the other capabilities of IO. No changes would need to be made to the organization. Currently, the service level network monitoring activities are responsible to the JTF-CNO. Under the USIOC, this relation would stay the same, as the aforementioned activities would be under the command of the service level components, discussed earlier, that would be subordinate to the USIOC. At this time, the JTF-CNO is responsible for CND and CNA functions. In the original

model for providing IO, the CNA functions were separated from the CND functions, but this is not a mandatory separation as long as the IOCERT maintains deployable CNA teams capable of supporting combat support packages. As well, the CND teams would need to be deployable to support incident response in the case of a detected intrusion. It is unknown if the JTF-CNO maintains legal and law enforcement functions within its organization, but if not, these functions would need to be added. The goal of the IOCERT is to form a single integrated capability to defend against network attacks and to attack the network of an opponent. In order to accomplish this, the service level components and any JTF functions must be subordinate to a unified agency such as the IOCERT.

I. DIVISIONAL LIAISONS

The function of a divisional liaison capability is to ensure the units supported, in this case the combatant commanders, have an avenue to relay their needs to the commander of the USIOC. It is a means for the commander of the USIOC to ensure his or her people "on the scene" are meeting the requirements of the supported unit or command. In the USIOC, this function would be accomplished by creating IO commands (IOC) within the regional commands. This is similar to the USSOCOM model where individual Special Operations Commands are established in the regional or combatant commands. As with the USSOCOM model, the IOC commanders would be subordinate to the combatant commander but would receive funding and administrative guidance from the USIOC. Similar to the JFC, this would reduce a combatant commander's staff by providing a single focal point for the J2 and J6 functions. As well, these IOC commanders would be the conduit for passing operational plans to functions under support within the USIOC, i.e., JWAC and JSC. Additionally, these commanders would work with the Product Development and Distribution function within the USIOC to ensure the systems being developed meet the needs of the combatant commander. The IOC commanders would also provide the conduit for request a combat support package during a time of crisis or hostility. In short, the IOC commanders would facilitate the ability of the USIOC to meet the combatant commander's IO needs for both peace and wartime.

J. INTERRELATION WITH OTHER DOD AGENCIES

1. Defense Information Systems Agency (DISA)

The USIOC and its service level components would be the bridge between DISA and the rest of DOD. In this function, the USIOC would facilitate agreements for backbone access to the defense information infrastructure during both peace and wartime. DISA's DOD CERT would be consolidated with the IOCERT, as these two functions would form an unnecessary redundancy if they both existed.

2. National Reconnaissance Office (NRO)

The relationship between the NRO and the DOD would not change under the USIOC concept. The only change would be that the information NRO currently provides the DOD would flow through the USIOC and its subordinate units, since the USIOC would control the intelligence assets within the DOD.

3. National Security Agency (NSA)

As with the NRO, the only change between the NSA and the DOD would be that the information provided by NSA would flow through the USIOC and its subordinate assets.

4. Defense Intelligence Agency (DIA)

As with the NSA, the only change between the DIA and the DOD would be that the information provided by the DIA would flow through the USIOC and its subordinate assets.

5. Chairman Joint Chiefs of Staff (CJCS)

Currently, the CJCS is tasked with ensuring the C4I needs of the combatant commanders are met. With the creation of the USIOC, the commander of the USIOC would be given this task. This allows the individual most equipped with the ability and assets to fulfill the task at hand. In other words, the individual that controls the assets and development of such assets would be the one ensuring the asset requirements of the combatant commanders are met.

K. CONCLUSION

This chapter has attempted to demonstrate the feasibility of actually implementing the generic organizational structure depicted in the previous chapter. In addition to

feasibility, the effort has been made to describe some of the cooperative benefits that can be gained by implementing such a structure.

The creation of the USIOC makes a great deal of sense from both a material and operational point of view. It would allow the development of IO related capabilities without the worry of unnecessarily redundant capabilities being created because "no one is in charge" of the overall IO picture. As well, an USIOC would bring various support functions under one roof to ensure unity of effort, command, and application. Such a capability would allow operational commanders of the combat variety the ability to focus on the area they are most qualified to focus on, which is what direct force assets to utilize in order to achieve victory. With the creation of the USIOC, the combatant commander would no longer have to focus on what to strike, what are the ramifications of hitting a specific target, how to communicate with higher echelon, merely how to apply direct force to best achieve mission accomplishment.

VI. MODELING THE MODEL: A CULTURE OF KNOWLEDGE

A. INTRODUCTION

The purpose of this chapter is to demonstrate the gains that can be realized by working within a community such as the one that would be created if the IOC were established. This demonstration is accomplished by modeling an abstract organization derived from the description of an IO cell as described in Joint Pub 3-13, Joint Doctrine for Information Operations. The modeling software used here is Vite©. Vite© has been used to demonstrate the quantitative difference in accomplishing the creation of an IO plan between team members with varying skills and skill levels. Two scenarios are used. The first scenario uses team members who have a high degree of skill in their individual specialty, but a low degree of skill in other areas. Such a scenario would be similar to a situation that would exist if a JTF were formed, and various people who had not worked together in creating an IO plan were thrown together for such a purpose. In contrast, the second scenario simulates a situation where the individuals working together on an IO plan have a high degree of expertise in their given specialty and a medium degree of expertise in the other specialty areas. This medium degree of specialty is based on the existence of an IOC, in which the personnel involved in IO planning would have worked and exercised together prior to the creation of the JTF. In other words, the second scenario attempts to simulate the gains that can be realized by having people work together in an organization and benefit from cross knowledge and thus develop a common understanding or a culture of knowledge.

B. ABOUT VITE

Vite© is a commercially developed simulator that is based on research accomplished at Stanford University (Vite©, 1996). Using Vite©, managers are able to design organizations by building and analyzing computational models of planned organizations and the processes that they support. As well, it can be used to consider the details involved with project performance and compare these details against modified versions of the organization. This is accomplished by linking a project plan, an organization, and a simulator that uses discrete event simulation to simulate project

accomplishment. Graphical outputs provide such information as: predicted time to complete the project, the total amount of effort involved, and various other measures of project quality. The conceptual framework of the simulation consists of an activity model, an actor model, and the simulator. Activity models represent the projects or products the organization is accomplishing. As well, each activity requires a primary skill necessary for accomplishing the activity. The "actors" are the personnel involved in product or project accomplishment. Each "actor" is assigned one to many skills with the degree of expertise for each skill capable of being set to high, medium, or low. As well as simulating actors executing or working on activities, the simulator also simulates information exchanges between activities. This functionality is needed when information from one activity is needed in the execution of a separate activity.

C. MODEL OVERVIEW

As stated previously, this chapter focuses on attempting to model a portion of the proposed IOC to demonstrate the benefits that can be realized by creating a single organization that focuses on the realm of IO. To that end, two scenarios of a cell attempting to develop an IO plan for a JTF are modeled. Such a cell would nominally be a subset of the combat packages within the IOC that would support a JFC. This section covers the similarities between the two scenarios, i.e., the activities, the actors, and information exchanges.

1. The Actors

The actors simulated in the model are the IO Officer, Intel Officer, PSYOP Officer, CNA Officer, EW Officer, PA Officer, CA Officer, and Legal Officer. Each of these actors is responsible for an individual process or product. Each actor has a varying degree of skill in the following areas: Intel, PSYOP, Communications (used for CNA), PA, CA, EW, Legal and IO.

2. The Activities

The activities simulated are: IO Plan, Intelligence (Intel) Product, Rules of Engagement (ROE), Psychological Operations (PSYOP) Plan, Computer Network Attack (CNA) Plan, Electronic Warfare (EW) Plan, Public Affairs (PA) Plan, and Civil Affairs (CA) Plan.

a. IO Plan

The IO Plan is the consolidated plan for the JTF and requires skill in IO. It consists of the PSYOP Plan, the CNA Plan, the EW Plan, the PA Plan, and the CA Plan. The fact that the IO plan is an integration of the various other plans is represented in the simulation by information exchanges between the various singular activities and the IO plan. As well, these information exchanges represent the process of ensuring the various plans work together in a synergistic manner. By synergistic, it is meant that the plans do not conflict with each and represent a single, consolidated, and collaborative approach to IO. The actor responsible for the IO Plan is the IO Officer, who is also in charge of all the other actors. The main purpose of the IO Plan activity is to simulate the management and leadership process executed by the IO officer.

b. Intel Product

The Intel Product activity simulates the process of gathering the relevant intelligence needed to develop the various individual products and the overall IO Plan and requires the skill of Intel. For the purpose of the model, it is assumed that all that is required for accomplishing this activity is gathering existing intelligence data. In other words, this activity does not represent the actual gathering of intelligence through various sensor platforms, be they electronic or human. The actor responsible for developing the Intel Product is the Intel Officer. Information exchanges are modeled between the Intel Product, the PSYOP Product, the CNA Product, and the EW Product. The rationale for these information exchanges is that those various products will need intelligence data to determine targeting data and means of attack based on the target and any associated defenses.

c. ROE

The ROE Product simulates the process of determining the legal targets and means of attacks based on the commander's intent and the available list of targets, and it requires legal skills. The actor responsible for this activity is the Legal Officer. Information exchanges exist between the ROE Product and the PSYOP Plan, the CNA Plan, the EW Plan, and the PA Plan. The rationale for these information exchanges is similar to the information exchanges for the Intel Product in that these various products

will need to know what targets and means of attack are legal per the commander and existing national and international law. For the exchange with the PA Plan, the rationale is that the PA Plan will need to account for what is and what is not releasable information.

d. PSYOP Plan

The PSYOP Plan activity simulates the development of a traditional PSYOP Plan and requires the skill of PSYOP. For the purpose of the model it is assumed that a National Command Authority approved plan does not exist and that the approval authority has been delegated to the JFC. The actor responsible for this activity is the PSYOP Officer. Information exchanges exist between the PSYOP Plan and the CNA Plan, the EW Plan, and the PA Plan. The rationale for the information exchanges between the PSYOP Plan and the CNA Plan is that these two plans will need to know not only the operational impact of successful attacks against their respective targets, but the psychological impact as well. Similarly, the PSYOP Plan will have to account for the change in the target audience's mindset as a result of successful EW and CNA attacks. The information exchange with the PA plan is needed for the purpose of perception management conflicts. For example, if the PSYOP Plan involves convincing a target audience that a given situation is X, then the PA Plan, through information releases, would not want to give the perception that the situation is actually Y, where X and Y are not coherent.

e. CNA Plan

The CNA Plan activity simulates the creation of a CNA Plan and requires the skill of communications. The actor responsible for the CNA Plan is the CNA Officer. As previously stated, an information exchange exists between this plan and the developed ROE because the creators of the CNA plan will need to know the legalities involved with specific targets and means of attack. Additionally, an information exchange exists between the CNA Plan and the EW Plan. The rationale for this information exchange is to ensure that the two plans do not overlap regarding intended targets. For example, if the CNA plan involves an attack against an integrated enemy air defense system, one would not want an EW attack to result in the destruction of the system, thus preventing a CNA that could conceivably co-opt the system. By exchanging information, the actors

involved with the two plans can collaborate and ensure a single cohesive plan that achieves optimal results.

f. EW Plan

The EW Plan activity simulates the creation of an EW Plan and requires the skill of EW. The actor responsible for the EW Plan is the EW Officer. The only information exchanges for the EW Plan are the previously mentioned exchanges between the IO Plan and the CNA Plan.

g. PA Plan

The PA Plan activity simulates the creation of a PA Plan beyond the traditional PA plan of hosting media sources and coordinating information releases and requires the skill PA. Due to the information exchanges previously mentioned with ROE and the PSYOP Plan, this activity attempts to simulate a PA Plan that practices perception management. In other words, this activity attempts to simulate the creation of a plan that would not only satisfy the media's thirst for information, but would also attempt to shape public opinion in a manner conducive to the overall goals of the campaign and related operations. In this vein, an additional information exchange exists between the PA Plan and the CA Plan. The rationale for this exchange is so the activities of the CA Plan can be incorporated into the PA Plan. Then PA personnel can release information that could potentially cast a positive light on the JTF and its associated coalition or governmental body.

h. CA Plan

The CA Plan activity simulates the creation of a traditional CA Plan and requires CA skills. The actor responsible for the CA Plan is the CA Officer. Information exchanges between the CA Plan and the PA and IO plans have been addressed previously.

3. Activity Flow

The flow of activities is determined by establishing a successor activity for each activity. In this model the activities start when the commander's intent is received. Once this intent is received, work begins on developing the overall IO Plan and the Intel Product. Work beginning on the IO Plan is merely representative of the IO Officer

beginning the planning process. Once the Intel Product is complete, work begins on the CA Plan, PSYOP Plan, and ROE. To reduce potential conflict between the PSYOP Plan and the PA Plan, the PA Plan begins after the PSYOP Plan is completed. Similarly, work does not begin on the CNA Plan and EW Plan until the ROE is complete so the legality of targets can be determined. After the ROE is completed, work begins on the CNA Plan and EW Plan, which once completed go to the end of the process, called execution. Likewise, once work begins on the PA Plan, which started after completion of the PSYOP Plan, the PA Plan goes to execution. Also, the IO Plan and CA Plan go to execution once completed. The integration of the various plans into a comprehensive IO plan is simulated via the previously mentioned information exchanges. Finally, each activity takes five days to complete with the exception of the IO Plan, which takes 15 days in an ideal environment. These durations were selected arbitrarily, but remain the same in both scenarios to ensure comparable results.

4. The Model

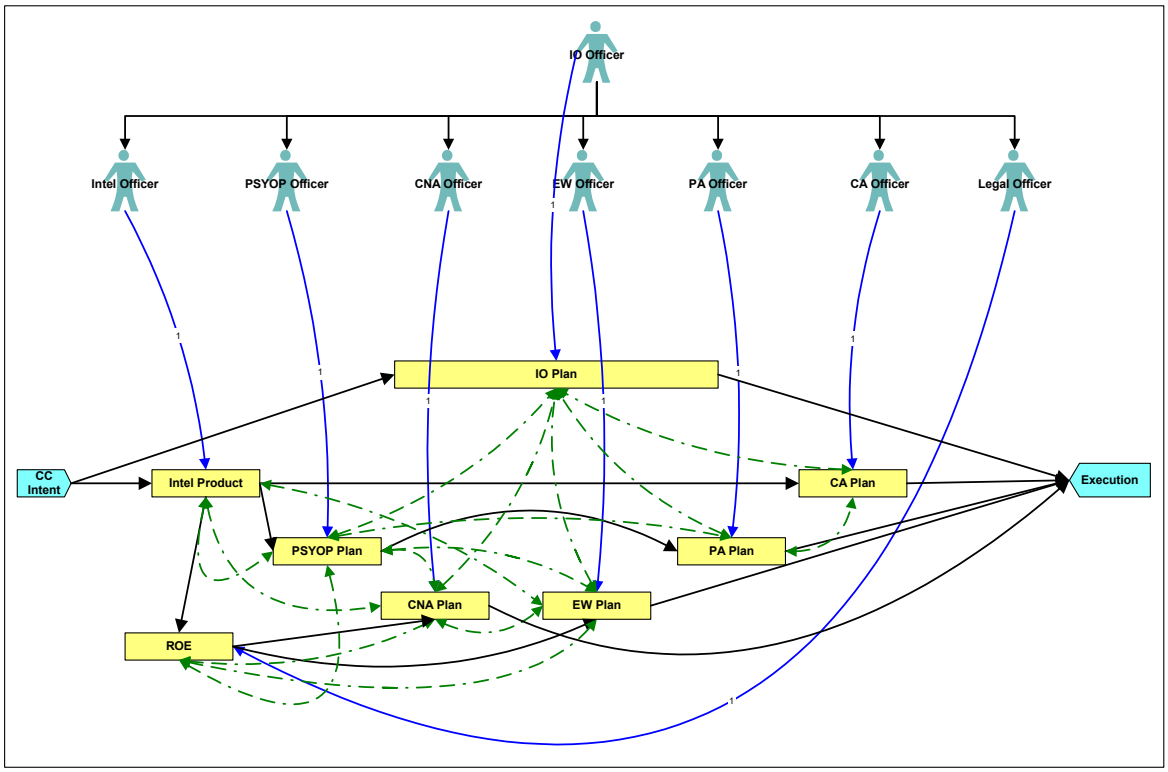

Figure 15. IO Cell Vitae© Model

The model described is depicted in Figure 15. The lines leading from the actors at the top of the model to the activities in rectangles at the bottom represent the assignment of actors to activities. The solid lines leading from activity to activity indicate activity succession, with the arrow designating the successor of a previous activity. The dashed lines between activities indicate information exchanges between activities. Finally, the overall process starts with "CC Intent" and ends with "Execution".

The key to the model is the information exchanges. Where there is an information exchange between two activities, the degree of success for the exchange will depend on the skills of the actor. For example, the exchange of information between the ROE and PSYOP Plan products will depend on the ability of the actors to understand what others are working on. If the PSYOP Officer has some level of understanding regarding the Intel Officer's skill, which was used to create the ROE product, then the information exchange will go smoothly. In effect, a real world scenario of a PSYOP Officer and an Intel Officer carrying on a conversation is being modeled. The more the two players have in the way of common knowledge, the easier their ability to communicate will be. A high degree of this simulated ability to communicate can result in the overall process being accomplished in less than the specified 15 days; conversely, a low degree of simulated communication ability can cause the overall process taking in excess of the specified 15 days.

D. SCENARIO 1

As previously stated, scenario 1 simulates various personnel being drawn together to develop an IO Plan for a JTF. For the purpose of the simulation, it is assumed these people have never worked together in a collaborative environment before. This scenario models a typical situation where diverse individuals from diverse career fields have come together for the purpose of IO planning.

1. Skill Levels

The assumption is made that, since these individuals are not members of a single organization, they have a low degree of expertise in the other's career field. Since current doctrine requires that the IO Officer come from the operations community, it is assumed that the IO Officer only has a medium degree of skill in IO. Finally, it is

assumed that all the actors in scenario 1 have a low level of experience in the application of developing an IO Plan. Table 2 depicts the various skill levels of the actors in scenario 1.

Actor / Skill	IO Officer	Intel Officer	PSYOP Officer	CNA Officer	EW Officer	PA Officer	CA Officer	Legal Officer
IO	Medium	Low	Low	Low	Low	Low	Low	Low
Intel	Low	High	Low	Low	Low	Low	Low	Low
PSYOP	Low	Low	High	Low	Low	Low	Low	Low
Comm	Low	Low	Low	High	Low	Low	Low	Low
EW	Low	Low	Low	Low	High	Low	Low	Low
PA	Low	Low	Low	Low	Low	High	Low	Low
CA	Low	Low	Low	Low	Low	Low	High	Low
Legal	Low	Low	Low	Low	Low	Low	Low	High

Table 2. Scenario 1 Skill Levels

2. Results

The results for simulating scenario 1 are depicted below in Table 3. The overall length of time taken to develop the IO Plan was 43 days. Due to the lack of common knowledge between the players, some tasks have taken longer than the allotted five days due to an inability to efficiently exchange information.

Scenario 1 Activity	Assigned To	Simulated Start	Simulated Duration
CC Intent		21-Mar-02	
Intel Product	Intel Officer	21-Mar-02	9 Days
IO Plan	IO Officer	21-Mar-02	43 Days
ROE	Legal Officer	30-Mar-02	2 Days
PSYOP Plan	PSYOP Officer	30-Mar-02	10 Days
CA Plan	CA Officer	30-Mar-02	9 Days
CNA Plan	CNA Officer	2-Apr-02	2 Days
EW Plan	EW Officer	2-Apr-02	10 Days
PA Plan	PA Officer	10-Apr-02	9 Days
Execution		3-May-02	

Table 3. Scenario 1 Results

E. SCENARIO 2

As previously stated, scenario 2 simulates personnel from an existing IOC being tasked with developing an IO Plan for a JTF. For the purpose of the simulation, it is assumed that these people work together in a day-to-day environment and engage in routine wargaming exercises that involve the development of an IO Plan.

1. Skill Levels

Due to the fact that these actors work together in a day-to-day environment, it is assumed that they have a medium degree of skill in one another's career field. As well, since the individuals modeled in scenario 2 engage in wargaming exercises, it is assumed that they have a high degree of experience in the application of developing an IO Plan. Table 4 depicts the various skill levels of the actors in scenario 2.

Actor / Skill	IO Officer	Intel Officer	PSYOP Officer	CNA Officer	EW Officer	PA Officer	CA Officer	Legal Officer
IO	High	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Intel	Medium	High	Medium	Medium	Medium	Medium	Medium	Medium
PSYOP	Medium	Medium	High	Medium	Medium	Medium	Medium	Medium
Comm	Medium	Medium	Medium	High	Medium	Medium	Medium	Medium
EW	Medium	Medium	Medium	Medium	High	Medium	Medium	Medium
PA	Medium	Medium	Medium	Medium	Low	High	Medium	Medium
CA	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium
Legal	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High

Table 4. Scenario 2 Skill Levels

2. Results

The results for simulating scenario 2 are depicted below in Table 5. The overall length of time taken to develop the IO Plan was 14 days. Due to the common knowledge between the players, some tasks have been accomplished prior to the allotted five days due to efficient information exchanges.

Scenario 2 Activity	Assigned To	Simulated Start	Simulated Duration
CC Intent		21-Mar-02	
Intel Product	Intel Officer	21-Mar-02	4 Days
IO Plan	IO Officer	21-Mar-02	14 Days
ROE	Legal Officer	25-Mar-02	1 Day
PSYOP Plan	PSYOP Officer	25-Mar-02	5 Days
CA Plan	CA Officer	25-Mar-02	4 Days
CNA Plan	CNA Officer	26-Mar-02	1 Days
EW Plan	EW Officer	26-Mar-02	5 Days
PA Plan	PA Officer	30-Mar-02	4 Days
Execution		5-Apr-02	

Table 5. Scenario 2 Results

F. ANALYSIS

The immediate analysis of the simulations is that scenario 2 supports the assertion that personnel from an organization who have knowledge of one another's varying skills are more able to develop a timely product than personnel who have no familiarity with each other's skill sets. However, this assertion can easily be argued against based on the fact that the single activity driving overall task duration in each scenario was the IO Plan. Furthermore, the IO Officer in scenario 1 had a medium skill level in his primary skill, IO, and a low level of experience in developing an IO Plan. The combined effect would be that the IO Officer was the cause of the elongated task duration in scenario 1. Thus, the argument could be made that by merely training IO Officers, the military could improve its capability to do IO planning and would not need to create an organization to promote a culture of knowledge. Based on this proposed argument, it is necessary to compare the activity durations with each scenario individually to see if there is a quantitative advantage to be gained from having an organization that provides a culture of knowledge. Table 6 illustrates the differences in activity duration between the individual activities and provides a percentage improvement from scenario 1 to scenario 2.

Scenario Activity	Assigned To	Simulated Duration - Scenario 1 in Days	Simulated Duration - Scenario 2 in Days	Duration Deltas	Improvement %
CC Intent					
Intel Product	Intel Officer	9	4	5	55.56%
IO Plan	IO Officer	43	14	29	67.44%
ROE	Legal Officer	2	1	1	50.00%
PSYOP Plan	PSYOP Officer	10	5	5	50.00%
CA Plan	CA Officer	9	4	5	55.56%
CNA Plan	CNA Officer	2	1	1	50.00%
EW Plan	EW Officer	10	5	5	50.00%
PA Plan	PA Officer	9	4	5	55.56%
Execution					

Table 6. Scenario Analysis

As shown in Table 6, each area showed a minimum 50 percent improvement in regards to task duration from scenario 1 to scenario 2. As a reminder, the only difference between the skills of the actors from scenario 1 to scenario 2 was that each actor went from a low to medium level of skill in his counterpart's skill area and from a low to high level of experience in regard to the application of building his portion of a consolidated IO Plan. This is in line with the guidance provided in the Vite© software that states little experience and excellent skill indicate the application experience be set to low and the skill level be set to high, as was the case in scenario 1. In scenario 2, the skill and application levels were both set to high, which is once again in line with the guidance provided in Vite©, which states that lots of experience and excellent skills indicate the application experience and skill level both be set to high.

G. CONCLUSION

The purpose of this chapter was to use commercial modeling software to determine if there were a quantitative difference between having individuals from an IO organization, as opposed to individuals who had no previous working relationship, accomplish a task. This was accomplished by having various actors with various skill sets accomplish the task of developing an integrated IO plan. Modeling the difference between the individuals from an organization and individuals with no previous working relationship was accomplished by varying the skill sets of the individual actors. For the personnel from an organization, their skill in areas outside their specific area of expertise

was increased based on the contention that working in a common environment would give them a better than casual familiarity with their peer's area of expertise. For the scenario in which the participants had not previously worked together, their skill in their peer's area of expertise was set to low based on the contention that the individual participant would have come from their own functional community and thus have had a low level of knowledge in their peer's area of expertise.

The results of the model provide strong support for having individuals from an organization who have a working knowledge of their peer's area of expertise accomplish a task. In the context of this thesis, the results of the model support the creation of an IO command that would foster the sharing of knowledge for the purpose of accomplishing IO related tasks. While this model only compared task durations as the metric for supporting the aforementioned contention, one can reasonably assume that the quality of an integrated product would increase as the knowledge of the various actors in the various skills required to develop the integrated product increased. While the IOC is not the only way to create such a community of knowledge, a benefit of the IOC would be a community of knowledge. In addition, if the IO cell came from an IO command that owned the intelligence gathering assets and data, then request for assistance from the cell would be like one-stop shopping where the storeowner has a vested interest in the shopper. In short, by creating an IO command, a community of knowledge can be created that would lend itself to the creation of timely and quality IO related products.

VII. CONCLUSION

A. SUMMARY

We have seen the inherent problems in the U.S. military's current approach to IO. First, the centralized direction which unity of command offers is clearly absent. This lack of unity also promotes individual objectives, direction and doctrine with little consolidation of effort across service-specific command lines and across the military services themselves. With little shared efforts in the military's approach to IO, the inevitable fallout is redundancy that increases the costs of moving forward in the information age. All these problems boil down to a deficiency in centralization. The centralization inherent in an established IO command will enable the U.S. military to form clear, comprehensive strategy with respect to IO.

There are some who are opposed to this revolutionary change. They claim that putting all information experts under a single command will effectively minimize and limit their ability to create and follow-through with needed IO concepts. In a way, IO techniques will fester within the new command and never flow to operational units. This is a valid concern, but safeguards have been built into the organizational structure specifically to prevent this. The proposed structure here will not allow such stagnation, especially in view of the proposed response teams and product development and distribution. Additionally, the organizational support will be provided in a matrix manner, driving the provider to balance customer concerns and higher command level's wishes. Even if stagnation is encountered there are appropriate avenues of feedback in place to counter such a standstill, such as the divisional liaisons implemented within the IOC.

As well as having safeguards against a purely inward focus that a large bureaucracy can tend to foster, the IOC, by design, has the tentacles necessary to ensure IO is used in every aspect of the military. For instance, were a unified IOC created, each regional CINC would have an IO component in the liaison position, i.e., IOCEUR. Not only would this position aid in making the functional IOC responsive to customer needs, it also ensures that IO is a viable tool available to the CINC on a day-to-day basis. By

having an everyday presence, which has accesses to a large functional pool of resources, the CINC's ability to utilize IO is greatly enhanced by the daily awareness of IO provided by the liaison position and associated staff. In other words, as opposed to monopolizing IO in a self-interested manner, the IOC ensures IO is dispersed throughout the military or individual service.

By utilizing Mintzberg's ideas, the U.S. military can utilize a centralized organizational approach that begins with emphasis at the strategic apex's formulation of strategy. This centralization does not cancel the opportunity to develop selective decentralization when needed, thus allowing for benefits of both centralization and decentralization. An example of this selective decentralization would be the support provided to units in the form of tailored packages as depicted in Figure 10. Feasibly, the make up of such tailored packages are in response to a customer's needs as opposed to the IOC's dictates. Therefore, as demonstrated, the structure can be organized in a way to meet the needs of individual units, but at the same time maintain a centralized theme.

Most of the goals of a new IO command can be successfully achieved by a mere centralized design. A clearly defined, single entity can provide concise, overall guidance for the U.S. military's approach to IO. This will allow the military to remain one step ahead of its adversaries in IO. We should not continue our ad hoc approach to information dominance, which in turn permits enemies to forge ahead as we continue the IO debate. The U.S. military needs to organize for victory in the information domain and it should do so by creating an innovative IO command.

B. FURTHER RESEARCH

Due to the constraints of time, there are some areas related to this thesis that were not thoroughly researched. As well, the very nature of academia, the generator of thesis requirements, demands that further research will always exist. In this vein, the below areas are some of the areas related to this thesis upon which further research would be helpful.

1. Classified Data

All of the research accomplished for this thesis was accomplished at the unclassified level. A reasonable argument could be made that to fully explore the diverse

areas that an IOC would be responsible for, one must delve into the classified realm. Such delving might reveal a more organized effort at implementing IO than what appears to be occurring based solely on unclassified information. Thus, the information in this thesis could be enhanced by the contribution of classified information that relates to the tactics, techniques, and procedures that currently exist within the IO realm.

2. Further Integration of Surveillance and Reconnaissance

Within the organization described in this thesis, the attempt has been made to create a strong integration of all the related fields of IO, i.e., intelligence, communications, PSYOP, civil affairs, etc. However, the connection of the proposed organization to the areas of surveillance and reconnaissance is weak at best. In today's military environment these two areas are an integral part of forming and measuring the results of an IO plan or campaign. By increasing the tie between a nominal IOC and surveillance and reconnaissance, it would be possible for a single entity to provide command and control of such assets. Were an IOC to be created at the unified command level, arguably this command and control could be provided without concerns regarding the parochialism of the individual services, as the unified command environment would provide the joint flavor necessary for truly joint operations.

As an example, in the application of the model the liaison officer function was implemented by creating theater commands such as IOCEUR. In order to facilitate the coordination of space-based surveillance and reconnaissance assets, it may be necessary to create a liaison between the USIOC and SPACECOM, i.e., IOCSPACE. Regardless, within this general area there is additional research that could be accomplished.

3. Manpower Study

The devil is in the details and with any major organizational proposals or changes one of the devils is manpower. For the purposes of this thesis, current organizations were used to demonstrate the feasibility of implementing the proposed organizational structure. Some of the existing organizations were identified as needing enhancement in certain areas in order to be fully functionally within a unified IOC. These enhancements would involve robbing some forces, which would necessarily require a manpower study to be done. Therefore, an additional area of needed research is manpower.

4. Fiscal Feasibility

If the first devil in organizational changes in manpower the other devil is money. Using existing organizations would hopefully minimize the monetary impact of implementing an IOC. This minimization, however, does not negate the requirement for a price tag associated with standing up the organization. Thus, a study on the fiscal feasibility would be an additional area of research regarding this thesis.

5. Flattening the Hierarchy

Within the military there is currently much discussion about whether the existing command structure can be simplified or flattened. One of the main drivers of this discussion is technology. The argument is that, based on the military's advances in telecommunications, there is no longer a need for the numerous layers that currently exist between the shooter and the top-level commander.

Assuming there is validity to such argument then an IOC organization would be a prime candidate for experimenting with a flatter hierarchy. The main reason for this contention is that technology will be at the core of the IOC, and if technology is the enabler for a flatter hierarchy, then the IOC would not need the huge bureaucratic command structure that is associated with most of today's military organizations. In order to determine the validity of this assumption, further research is necessary.

LIST OF REFERENCES

Adams, J. (1998). The Next World War: Computers Are the Weapons and the Front Line is Everywhere. New York: Simon & Schuster.

Adams, T. (1998). US Special Operations Forces in Action. Portland, Oregon: Frank Cass Publishers.

"Air Force Communications Agency." (2000, November). Air Force Communications Agency Fact Sheet. Retrieved January 21, 2001 from the World Wide Web: http://public.afca.scott.af.mil/public/afcafcts.htm.

"Air Intelligence Agency Merges With ACC." (2000, October27). AFPN. [Online]. Retrieved January 21, 2001 from the World Wide Web: http://www.af.mil/news/Oct2000/n20001027_001624.shtml.

Alberts, D. (1996). "Appendix D. Defensive Information War: Problem Formation and Solution Approach." Information Warfare and Deterrence. Washington, D.C: National Defense University Press. Retrieved May 25, 2001 from the World Wide Web: http://www.fas.org/irp/threat/cyber/docs/iwd/appd.html.

Alexander, B. (1995). The Future of Warfare. New York: W. W. Norton & Company, Inc.

Assistant Secretary of Defense (C3I). (2001,1 July). "What is the Overall Mission of ASD(C3I)?" Retrieved September 10, 2001 from the World Wide Web: http://www.c3i.osd.mil/faq/.

Builder, C. (1994). The Icarus Syndrome. New Brunswick: Transaction Publishers.

Department of the Army. (1996, August). " Chapter 6: Planning and Execution." Field Manual 100-6. Washington, D.C. Retrieved May 27, 2001 from the World Wide Web: http://www.fas.org/irp/doddir/army/fm100-6/ch6.htm.

Department of the Army. (1996, August). "Appendix B." Field Manual 100-6. Retrieved September 20, 2001 from the World Wide Web: http://www.adtdl.army.mil/cgi-bin/adtdl.dll/fm/100-6/appendb.htm.

Department of the Army. (1995, 1 August). "Military Operations: Concept for Information Operations." TRADOC Pamphlet 525-69. Fort Monroe, VA. Retrieved September 6, 2001 from the World Wide Web: http://www-tradoc.army.mil/tpubs/pams/p525-69.htm#terms.

Department of Defense. (2001, 1 June). Introduction to the United States Department of

Defense. Retrieved September 19, 2001 from the World Wide Web: http://www.defenselink.mil/pubs/dod101/whatwedo.html

DISA. (August, 1998). Contingency C4ISR Handbook for Integrated Planning. DIA Publications Dvision.

Fredericks, B. (1997). "Information Warfare: The Organizational Dimension." [Project]. Washington, D.C: Institute For National Strategic Studies. Retrieved May 22, 2001 from the World Wide Web: http://www.ndu.edu/inss/siws/cont.html.

Garamone, J. (2002, 28 February). "Rumsfeld Tells Troops to Expect the Unexpected." American Forces Press Service. Retrieved from the World Wide Web: http://www.hilltoptimes.com/story.asp?edition=42&storyid=997.

Garamone, J. (2002, 17 April). "U.S. Northern Command to Debut in October." American Forces Press Service. Retrieved from the World Wide Web: http://www.defenselink.mil/news/Apr2002/n04172002_200204175.html.

Goldberg, A. (1957). A History of the U.S. Air Force 1907-1957. Princeton, New Jersey: D. Van Nostrand Company, Inc.

Gortler, F. (1995, May). "Understanding Information Power and Organizing for Victory In Joint War Fighting." [Paper]. Quantico, Virginia: Marine Corps Command and Staff College. Retrieved May 26, 2001 from the World Wide Web: http://www.fas.org/spp/eprint/gortler.htm.

"Joint C4ISR Battle Center (JBC) Mission Brief." (May 23, 2001). Retrieved Septermber 12, 2001 from the World Wide Web: http://www.jbc.jfcom.mil/common/Public/Information/cmd_brf/index.htm.

Joint Chiefs of Staff. (1998, October). "Joint Doctrine for Information Operations." Joint Pub 3-13. Washingtion, D.C. Retrieved May 27, 2001 from the World Wide Web: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

"Joint Program Office – Special Technology Countermeasures (JPO-STC) Fact Sheet." (Date Unknown). Retrieved September 11, 2001 from the World Wide Web: http://www.nswc.navy.mil/IAP/jpo/mission.htm.

"Joint Spectrum Center (JSC) Mission." (November 27, 2000). Retrieved September 14 from the World Wide Web: http://www.jsc.mil/mission.asp.

"JITC Mission/Vision." (September 10, 2001). Retrieved September 20, 2001 from the World Wide Web: http://jitc.fhu.disa.mil/mission.htm.

"JTF-CNO Fact Sheet." (August 14, 2001). Retrieved September 20, 2001 from the World Wide Web: http://www.spacecom.af.mil/usspace/jtf-cno.htm.

Kreighbaum, J. (June, 1998). Force Application Planning: A systems-And-Effects-Based Approach. Air University Press. Retrieved September 12 from the World Wide Web: http://www.au.af.mil/au/database/projects/ay1998/saas/kreighbaum_jm.pdf.

Lerman, D. (2002, 3 February). "New Command Structure on Rumsfeld's Agenda." Retrieved from the World Wide Web: http://www.dailypress.com/news/columnists/dp-23395cm0feb03.column?coll=dp-news-columnists.

Marek, J. (2000, April). "Organizing to Win: Centralized Control for Information Warfare." [Research Project]. Maxwell AFB, Alabama: Air Command and Staff College. Retrieved May 3, 2001 from the World Wide Web: http://www.au.af.mil/au/database/projects/ay2000/acsc/00-109.pdf.

Marine Corps Combat Develop Command. (1998, May 15). "A Concept For Information Operations." Quantico, Virginia: U.S. Marine Corps. Retrieved May 5, 2001 from the World Wide Web: http://192.156.75.102/io/docs/iofinal.PDF.

Marquis, S. (1997). Unconventional Warfare: Rebuilding U.S. Special Operations Forces. Washington, D.C.: Brookings Institution Press.

Mintzberg, H. (1993). Structures in Fives: Designing Effective Organizations. New Jersey: Prentice Hall, Inc.

Morgan, J. (2000, November). "The Principles of War: A Look at Military Theory and Karl von Clausewitz." [Research Project]. Denver, Colorado: University of Denver. Retrieved May 26, 2001 from the World Wide Web: http://www.du.edu/~jamorgan/war/unit.

Nalty, B. (1997). Winged Shield, Winged Sword: A History of the United States Air Force. Washington, D.C.: U.S. Government Printing Office.

United States Space Command. (2001). JTF-CNO Homepage. Retrieved September 18, 2001 from the World Wide Web: http://www.spacecom.af.mil/usspace/jtf-cno.htm.

"Visions and Goals." (2000, October 10). Chief Information Officer Vision, Goals and Bottom Line. Retrieved January 21, 2001 from the World Wide Web: http://www.cio.hq.af.mil/public/public_vgbpage.shtml.

Vite© (1996-1999). ViteProject Windows NT/95/98 Version 2.2

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Dan Boger
   Naval Postgraduate School
   Monterey, California

4. Professor Erik Jansen
   Naval Postgraduate School
   Monterey, California

5. Jennifer Duncan
   Naval Postgraduate School
   Monterey, California